Nina Sorsa

TIETOJÄRJESTELMÄÄ UHKAAVIA TEKIJÖITÄ JA TIETOTURVA-KARTOITUS

Insinöörityö
Kajaanin ammattikorkeakoulu
Tekniikka ja liikenne
Tietoturvateknologia
Kevät 2011

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ
TIIVISTELMÄ

Koulutusala Tekniikka ja liikenne	Koulutusohjelma Tietotekniikka
Tekijä(t) Nina Sorsa	
Työn nimi Tietojärjestelmää uhkaavia tekijöitä ja tietoturvakartoitus	
Vaihtoehtoiset ammattiopinnot Tietoturvateknologia	Ohjaaja(t) Jukka Heino
	Toimeksiantaja Kajaanin ammattikorkeakoulu Tietohallinto / Risto Hyvönen
Aika Kevät 2011	Sivumäärä ja liitteet 41 + 17

Tämän insinöörityön toimeksiantajana on Kajaanin ammattikorkeakoulun tietohallinto. Työn tarkoituksena oli selvittää kohdeorganisaation tietoturvallisuuden tämänhetkinen taso.

Insinöörityöhön kuuluu teoreettinen osuus, jossa on kuvattu tietoturvallisuuteen liittyviä peruskäsitteitä ja määritelmiä. Tietoturvallisuus on jaettu osa-alueisiin, joissa jokaisen yhteydessä on kuvattu mahdollisia tietoturvauhkia ja keinoja niiden torjumiseksi. Teoreettisen osuuden pohjana on tietoturvastandardi BS7799-1:fi.

Teoriaosuuden lisäksi kohdeorganisaatiossa on tehty tietoturvakartoitus, joka on toteutettu haastattelemalla vastuullisessa asemassa olevia henkilöitä. Kysymykset haastattelua varten on laadittu teoriaosuuden perusteella.

Työn tuloksena saatiin selville Kajaanin ammattikorkeakoulun tietoturvallisuuden nykyinen tilanne. Kartoituksessa ilmenneistä puutteista on esitetty kehittämisehdotukset. Tässä insinöörityössä ei ole nähtävillä tietoturvallisuuden kehittämisehdotuksia, dokumentin luottamuksellisuuden vuoksi.

Kieli	Suomi
Asiasanat	tietoturvallisuus, tietoturvakartoitus
Säilytyspaikka	☒ Verkkokirjasto Theseus ☒ Kajaanin ammattikorkeakoulun kirjasto

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

THESIS
ABSTRACT

School School of Engineering	Degree Programme Information Technology
Author(s) Nina Sorsa	
Title Threats of the Information System and a Data Security Survey	
Optional Professional Studies Information security technology	Instructor(s) Mr Jukka Heino, Senior Lecturer
	Commissioned by Kajaani University of Applied Sciences Data Administrations / Risto Hyvönen
Date Spring 2011	Total Number of Pages and Appendices 41 + 17

This Bachelor´s thesis was commissioned by the Kajaani University of Applied Sciences' Data Administration.

The main purpose of this thesis was to examine the level of data security at Kajaani University of Applied Sciences, and to make some suggestions to improve it. This thesis contains two parts, public and confidential.

The first stage was to study good practices and instructions of data security, by using Standard BS7799-1 and other literature discussing data security and information technology. Some common threats are also mentioned. As a result of this study the first part of this thesis was created, it is the theory part, which contains public information about data security.

Next the level of data security at Kajaani University of Applied Sciences was studied. The study was made by interviewing persons in Data Administration and other departments. Observation was also used. As a result of this study the second part of this thesis was created. It contains only confidential material and is not published.

Language of Thesis	Finnish
Keywords	Data security, Information security
Deposited at	☒ Electronic library Theseus ☒ Library of Kajaani University of Applied Sciences

ALKUSANAT

Insinöörityön aihe tuli esille suorittaessani koulutukseen kuuluvaa pakollista harjoittelujaksoa Kajaanin ammattikorkeakoulun tietohallinnossa. Työhön liittyy teoreettinen osuus, jossa kerrotaan yleisellä tasolla tietojärjestelmiä uhkaavista tekijöistä sekä käytännön osuus, jossa kartoitettiin Kajaanin ammattikorkeakoulun tietoturvallisuuden tasoa.

Haluan kiittää Kajaanin ammattikorkeakoulun tietohallinnossa työskenteleviä asiantuntijoita mukavasta yhteistyöstä ja arvokkaista tiedoista sekä myös muita kartoitusta varten haastateltuja henkilöitä. Kiitokset haluan osoittaa myös työn ohjaajalle Jukka Heinolle ohjeista ja kommenteista sekä kielellisistä ohjauksista Eero Soiniselle ja Kaisu Korhoselle.

SISÄLLYS

SYMBOLILUETTELO

AD	(Active Directory). Sisältyy Microsoft Windows Server -käyttöjärjestelmiin. Sisältää tiedot käyttäjistä, tietokoneista ja verkon resursseista sekä mahdollistaa niiden keskitetyn hallinnan.
Algoritmi	Matematiikkaan ja tietojenkäsittelyyn liittyvä tarkoin määritelty joukko käskyjä tai ohjeita, joita käytetään ongelman ratkaisuun.
Footprinting	Järjestelmää kohtaan hyökkäävän tahon järjestelmällinen tietojen kerääminen kohdeorganisaatiosta. Tarkoituksena on luoda täydellinen profiili organisaation turvallisuustilanteesta.
Keylogger	Piilotettu ohjelma tai pienikokoinen laite, joka tallentaa näppäinten painallukset. Käyttäjätunnusten ja salasanojen urkkimiseen.
MAC-osoite	(Media Access Control) Verkkokortille tehtaalla fyysisesti kirjoitettu osoite, joka yksilöi verkkosovittimen ethernet-verkossa.
SIM	(Subscriber Identity Module) Matkapuhelimen älykortti ja tietovarasto, joka mahdollistaa matkapuhelinverkon käytön ja yhteystietojen ja tekstiviestien tallennuksen.
SSH	(Secure Shell) Salatussa tietoliikenteessä käytetty protokolla.
UPS	(Uninterruptible Power Supply) Varavirtajärjetelmä, jolla taataan tasainen virransyöttö lyhyiden sähkökatkosten aikana sekä tasataan jännitteen epätasaisuuksia.
USB	(Universal Serial Bus) Tiedonsiirtoväylä, jolla voidaan liittää esimerkiksi näppäimistö, hiiri tai muistitikku tietokoneeseen virtaa katkaisematta.
VPN	(Virtual Private Network) Yksityinen virtuaaliverkko, jonka avulla on mahdollista muodostaa turvallinen yhteys kahden erillään olevan tietokoneen välille Internetin kautta.

1 JOHDANTO

Tietoturvan tai oikeammin tietoturvallisuuden tarkoituksena on suojata organisaation tietojärjestelmä ja siihen tallennetut tiedot, organisaation palvelut ja tietoliikenne. Tietojärjestelmää ja sen turvallisuutta uhkaavat esimerkiksi erilaiset huijausyritykset, yksityisyyden loukkaukset, roskaposti, vakoilu ja virukset. Teknisillä ratkaisuilla tietoturvallisuutta pystytään pitämään yllä melko pitkälle, mutta se ei yksistään riitä, vaan lisäksi tarvitaan myös huolellisuutta käyttäjien taholta. Tietojärjestelmien käyttäjillä on jokaisella velvollisuus ottaa tietoturvallisuus huomioon omalta osaltaan jokapäiväisissä toimissaan ja siten osallistua koko järjestelmän suojaamiseen. Ihminen on kuitenkin yleensä se heikoin lenkki, joka voi aiheuttaa vahinkoa tietojärjestelmälle joko tahallisesti tai huomaamattaan.

Jokaisella yrityksellä tai organisaatiolla on hallussaan tietoa, joka on organisaation toiminnalle elintärkeää, eikä saa missään tapauksessa joutua muiden tahojen haltuun. Jokaisen organisaation tulee itse määritellä, millainen tieto on ehdottomasti pidettävä suojassa ulkopuolisilta. Tietoturvallisuudesta huolehtiminen varmistaa organisaation toiminnan jatkuvuuden. Suojattavia tietoja ovat asiakas- ja tuotekehitystiedot, liiketoiminta- ja tuotantotiedot sekä tiedot myynneistä, henkilöstöstä, markkinoinnista ja organisaation tietojärjestelmästä.

Tässä insinöörityössä käsitellään tietoturvallisuuden perusperiaatteita ja -käsitteitä sekä tietojärjestelmää uhkaavia tekijöitä ja suojautumista niitä vastaan. Tämän teoriaosuuden lisäksi on tehty myös tietoturvakartoitus Kajaanin ammattikorkeakoulun tietohallinnolle. Kartoituksen tuloksia ei tietojen luottamuksellisuuden vuoksi käsitellä.

Kajaanin ammattikorkeakoulu on Kajaanin kaupungin omistama liikelaitos, joka perustettiin vuonna 1992. Ammattikorkeakoulussa on opiskelijoita noin 2000 eri koulutusaloilla ja henkilökuntaa noin 180, josta opettajia noin 100. Kajaanin ammattikorkeakoulussa on viisi koulutusalaa, joista valmistuu ammattilaisia yhteiskuntatieteiden, liiketalouden ja hallinnon alalla, luonnontieteiden alalla, tekniikan ja liikenteen alalla, sosiaali-, terveys ja liikunta-alalla sekä matkailu-, ravitsemis- ja talousalalla. Koulutusohjelmia on 12, joista kolmessa opetus tapahtuu englanninkielellä. [1.]

2 TIETOTURVALLISUUDEN PERUSPERIAATTEITA JA MÄÄRITELMIÄ

Tässä luvussa mainittujen seikkojen lähteenä on käytetty Hakalan, Vainion ja Vuorisen kirjoittamaa Tietoturvallisuuden käsikirjaa [2].

Kirjallisuus ja eri tahojen julkaisemat standardit määrittelevät tietoturvallisuuden hieman eri tavoin, mutta kuitenkin perusajatuksena on, että tieto on organisaation tärkein omaisuus, jota on suojeltava luvattomalta käytöltä ja tarpeettomalta muuttumiselta. Tiedon on oltava luotettavaa, helposti saatavilla, oikeassa muodossa sekä pelkästään niiden henkilöiden saatavilla, jotka ovat siihen oikeutettuja.

Suojattavan tiedon lisäksi määritelmää on nykyisin laajennettu koskemaan myös tietojen käsittelyssä käytettäviä laitteistoja ja tietoliikennejärjestelmiä. Laitteistot ovat yleensä melko kalliita ja ne on syytä suojata luvattomalta käytöltä, vaikka luvaton käyttäjä ei olisikaan kiinnostunut organisaation tallennetusta tiedosta.

Klassisen tiedon arvoon perustuvan määritelmän mukaan tietoturvallisuus jaetaan kolmeen osatekijään: luottamuksellisuus, käytettävyys ja eheys. Nykyaikana tätä määritelmää pidetään kuitenkin liian suppeana, koska siinä ei huomioida laitteistojen ja tietojärjestelmien arvoa eikä tiedon tuottajaa tai omistajaa. Niinpä laajennetussa tietoturvallisuuden määritelmässä on edellä mainittujen kolmen osatekijän lisäksi kiistämättömyys ja pääsynvalvonta.

Joissakin yhteyksissä määritelmissä on myös mainittuna autenttisuus kuudentena tietoturvallisuuden osatekijänä. Autenttisuuden katsotaan olevan luottamuksellisuuden ja kiistämättömyyden perusedellytys, ja siitä syystä se on yleensä jätetty pois määritelmistä. Autenttisuuden varmistamisen tarkoituksena on järjestelmän käyttäjien ja tiedon käsittelyyn osallistuvan laitteiston luotettava tunnistaminen eli autentikointi (authentication).

2.1 Luottamuksellisuus

Luottamuksellisuus (confidentality) tarkoittaa sitä, että tietojärjestelmään tallennettuja tietoja pääsee katsomaan vain sellainen henkilö, joka on oikeutettu tietoja tarkastelemaan [2]. Yleensä ottaen työntekijän tulee päästä käsiksi vain sellaiseen tietoon, mitä hän tarvitsee välttämättä omassa työtehtävässään. Esimerkiksi organisaation työntekijöiden henkilö- ja palkkatietoi-

hin ei saa olla pääsyä muilla kuin henkilöstöhallinnossa sekä palkanlaskennassa työskentelevillä henkilöillä.

Luottamuksellisuutta ylläpidetään tietojärjestelmän laitteiden ja tietovarastojen suojaamisella käyttäjätunnusten, salasanojen ja käyttörajoitusten avulla. Myös erilaisilla salakirjoitusmenetelmillä pystytään parantamaan arkaluontoisen ja erityisen arvokkaan tiedon suojausta.

2.2 Käytettävyys

Käytettävyydellä (availability) tarkoitetaan tiedon saatavuutta tietojärjestelmästä. Tietojen tulee olla saatavissa oikeassa muodossa ja ilman turhaa viivytystä [2]. Erityisen tärkeää tiedon käytettävyys on esimerkiksi terveydenhuollossa. Kriittisessä tilanteessa potilaan tiedot perussairauksista ja käytettävästä lääkityksestä on saatava nopeasti ja niiden on oltava ajan tasalla.

Käytettävyyden takaamiseksi tulee huolehtia tieto- ja tietoliikennejärjestelmien laitteista siten, että ne ovat riittävän tehokkaita, ja käytössä olevat ohjelmistot ovat tallennetun tiedon käsittelyyn sopivia. Näiden lisäksi pyrkimyksenä on myös tiedon jalostuksen automatisointi mahdollisimman pitkälle. Tietojen tulee olla käyttäjän saatavissa haluamassaan muodossa.

2.3 Eheys

Eheydellä (integrity) tarkoitetaan sitä, että tietojärjestelmään tallennetut tiedot ovat paikkansa pitäviä eivätkä sisällä joko tahallaan tai tahattomasti aiheutettuja virheitä.

Eheyden ylläpidossa pääasiallisin vaikuttamiskeino on ohjelmistotekniset ratkaisut. Sovellusten ohjelmoinnin yhteydessä niihin asetetaan erilaisia rajoitteita, esimerkiksi syötettävän tiedon pituus voi olla rajoitettu tiettyyn merkkimäärään. Samalla voidaan ohjelmoida syötteen tarkistus, jolloin ohjelma tarkistaa, että syötetty tieto on juuri sellaista kuin pitääkin. Esimerkiksi numerokenttiin ei voi syöttää tekstiä ja päinvastoin. Myös varmistussummat ja tiivisteet ovat käyttökelpoisia tallennus- ja tiedonsiirto-operaatioiden yhteydessä.

Laitteiston osalta eheyden varmistamisessa virheiden estämiseksi käytetään esimerkiksi virheenkorjaavia muisteja ja väyliä. Tietoliikenneratkaisujen yhteydessä käytetään yleensä laitteita ja protokollia, jotka sisältävät virheen tunnistus- ja korjausmekanismeja.

2.4 Kiistämättömyys

Kiistämättömyydellä (non-repudiation) tarkoitetaan tietojärjestelmän ominaisuutta, jolla järjestelmää käyttävän henkilön tiedot tunnistetaan ja tallennetaan luotettavasti. Kiistämättömyyteen pyritään yleensä kahdesta syystä. Ensimmäisenä on halu varmistua tiedon alkuperästä ja toisena tilanteet, kun kyseessä on tietojen luvaton käyttö ja järjestelmän omistaja harkitsee juridisia toimia järjestelmän käyttäjää kohtaan.

Kiistämättömyyden varmistamiseen käytetään tunnistusmekanismeja, jotka liittyvät salausmenetelmiin, tai biometrisiä tunnisteita. Älykortit tai muut helposti mukana kuljetettavat pienet laitteet ovat yleisimpiä salaustekniikoita hyödyntäviä käyttäjätunnistusmenetelmiä. Älykorttiin tai muuhun vastaavaan laitteeseen tallennetaan käyttäjän henkilötiedot sekä sertifikaatti (certificate), joka on voimassa rajoitetun ajan. Biometrisessa tunnistuksessa on käytettävissä esimerkiksi laitteita, jotka tunnistavat käyttäjän sormenjäljen tai silmänpohjan perusteella.

2.5 Pääsynvalvonta

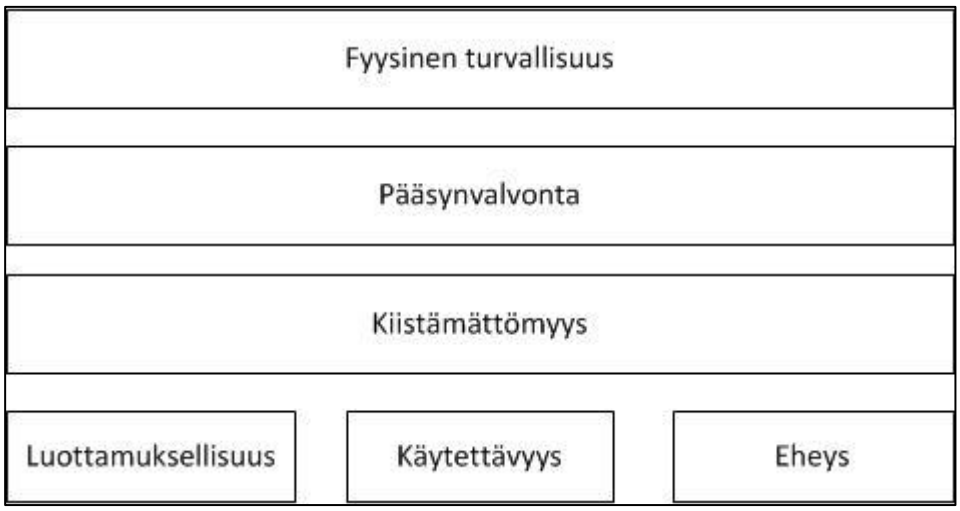
Pääsynvalvonta (access control) tarkoittaa eri menetelmiä, joilla pystytään rajoittamaan tietojärjestelmän käyttöä. Rajoitukset tietojen käytöstä kuuluvat luottamuksellisuuden ylläpitoon.

Organisaation tietojärjestelmä on yleensä tarkoitettu ainoastaan työtehtävien hoitamiseen. Organisaatiolle on tärkeää, että sen laitteistoja tai tietoliikennejärjestelmiä ei käytä kukaan ulkopuolinen tai oma henkilökunta omiin tarkoituksiinsa. Luvattomasta järjestelmän käyttämisestä aiheutuu ylimääräistä kuormitusta sekä laitteille että tietoliikenneverkolle. Ylimääräinen kuormitus saattaa heikentää järjestelmän käytettävyyttä.

Luvattomasta käytöstä saattaa aiheutua myös eheys- ja luottamuksellisuusongelmia. Luvattoman käytön seurauksena organisaation tietojärjestelmään voi päästä haittaohjelmia, jotka leviävät nopeasti koko järjestelmään.

Pääsynvalvontaan on kiinnitettävä huomiota entistä enemmän, koska nykyisin langattomat verkot ovat yleistyneet huomattavasti. Langattomia verkkoja pyritään käyttämään ulkopuolisten henkilöiden toimesta omaan Internet-liikenteeseen. Joissakin maissa nuorten suosimana harrastuksena on etsiä langattomia verkkoja ja murtaa niiden salaukset (war driving). Tarvittavat laitteet ja ohjelmat voi ostaa tietokonekaupoista tai tilata Internetistä.

Kuvassa 1 on nähtävillä tietoturvallisuuden osatekijät.



Kuva 1. Tietoturvallisuuden osatekijät

3 TIETOTURVALLISUUDEN OSA-ALUEET

Tietoturvallisuus jaetaan yleensä kahdeksaan eri osa-alueeseen. Turvallisuuden osa-alueiden jaottelun (hallinnollinen, fyysinen, henkilö, tietoaineisto, ohjelmisto, laitteisto ja tietoliikenne) avulla kokonaisuutta on helpompi käsitellä ja osa-alueiden perusteella laadittujen dokumenttien rakenne on selkeämpi. Tämän luvun pääasiallisina lähteinä on käytetty Tietoturvallisuuden käsikirjaa [2] ja standardia BS 7799-1:fi [4].

3.1 Hallinnollinen tietoturva

Hallinnollinen tietoturva on tietoturvallisuuden osa-alue, jonka avulla organisaation johto luo edellytykset tietoturvallisuuden kehittämiselle ja ylläpidolle. Pääasiallisena tarkoituksena on kaikkien tietoturvallisuuteen liittyvien asioiden yhdistäminen yhdeksi kokonaisuudeksi, jota on helppo hallita ja johtaa, samalla tavalla kuin esimerkiksi taloushallintoa tai henkilöstöhallintoa. Hallinnollista tietoturvaa tarkastellessa kiinnitetään huomiota organisaation toimintalinjauksiin ja periaatteisiin, johtamiseen ja resursointiin, toimintojen organisointiin sekä tietoturvallisuuden hoitoon liittyviin vastuisiin.

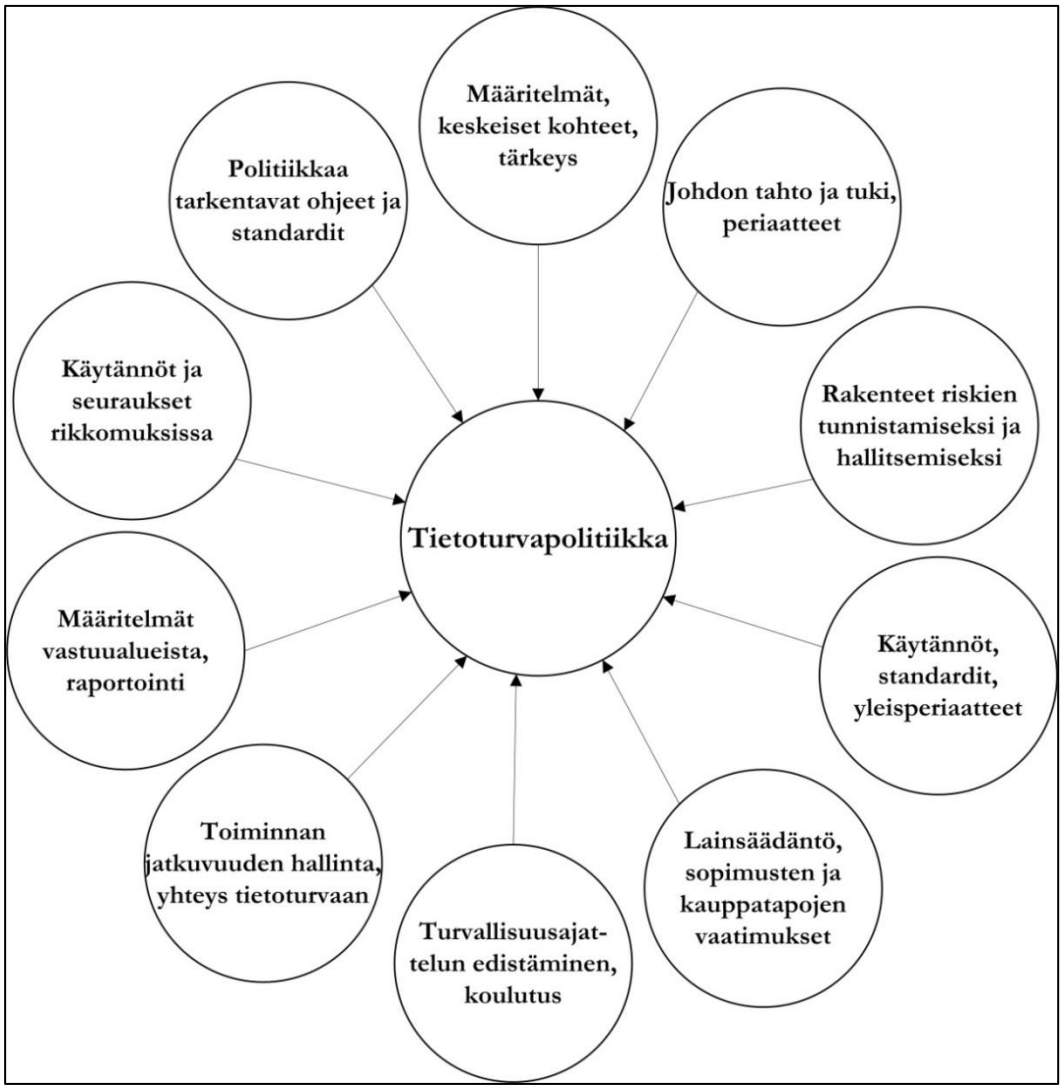
Organisaation tietoturvallisuuden toteutuksen pohjana on tietoturvapolitiikka (Information security policy), joka sisältää organisaation ylimmän johdon hyväksymät käytännöt, joiden avulla saavutetaan haluttu tietoturvallisuuden taso. Tietoturvapolitiikassa kuvataan yleisellä tasolla, mitä menetelmiä haluttuun turvatasoon pääsemiseksi on käytettävissä, mikä turvaamisaste on organisaation toimintaprosessien edellytys ja miten tietoturvallisuuden hallinnointi ja kehittäminen hoidetaan.

Tietoturvapolitiikan laadinta kuuluu organisaation ylimmälle johdolle. Tietoturvapolitiikka laaditaan kirjallisena, ja sen sisältämien ohjeiden tulisi olla käyttökelpoisia 5–10 vuoden ajan tietojärjestelmän ylläpitäjille ja toimintaprosesseista vastuussa oleville henkilöille. Vaikka tietoturvapolitiikka laaditaan suhteellisen pitkälle ajanjaksolle, tulisi sen sisältö tarkistaa vuosittain, jotta se vastaisi organisaation turvallisuustarpeita ja sen hetkistä toimintaa.

Tietoturvapolitiikka tulee laatia helposti ymmärrettävään muotoon, jotta myös muut kuin sen laatijat ja tietohallinto ymmärtävät sen sisällön. Dokumentti on tarkoitettu pääasiassa organi-

saatiossa työskenteleville henkilöille, mutta se voi olla myös osoitus tietoturvallisuuden hyvästä huolehtimisesta ja siten tärkeä markkinoinnin apuväline jaettavaksi esimerkiksi asiakkaille ja yhteistyökumppaneille. Monien isojen organisaatioiden tietoturvapolitiikka on suoraan nähtävillä julkisilla Internet-sivuilla. Dokumentti on yleensä julkinen, ja siitä syystä se ei saa sisältää arkaluontoisia tietoja. Liian yksityiskohtaiset kuvaukset teknisistä ratkaisuista ja käytänteistä voivat antaa arvokasta tietoa tietomurtojen suunnittelijoille tai muille hyökkääjille. Tarkemmat kuvaukset käytettävistä menetelmistä turvallisuustavoitteisiin pääsemiseksi tai menettelyistä rikkomusten yhteydessä lisätään tietoturvapolitiikan liitteiksi. Tämäntyyppiset liitteet luokitellaan joko luottamuksellisiksi tai salaisiksi, eikä niitä luovuteta kenellekään organisaation ulkopuoliselle henkilölle nähtäväksi.

Tietoturvapolitiikassa huomioitavat asiat ovat nähtävillä kuvassa 2.



Kuva 2. Tietoturvapolitiikan sisältö

Tietoturvapolitiikkaan kuuluvassa tietoturvasuunnitelmassa huomioidaan kaikki käytännön ratkaisut, joilla tavoiteltu tietoturvallisuuden taso pyritään saavuttamaan. Kirjallisessa muodossa olevassa suunnitelmassa määritellään tietojärjestelmässä käytettävät tekniset ratkaisut ja työmenetelmät yksityiskohtaisesti.

Tietoturvasuunnitelman voimassaolo on noin 2−5 vuotta, ja sen perustana ovat tietoturvapolitiikan asettamat vaatimukset ja periaatteet. Organisaation toiminnoissa tapahtuu muutoksia jatkuvasti, joko prosesseissa tai uuden teknologian käyttöönotosta johtuvia, joten suunnitelman päivittämisestä on huolehdittava säännöllisesti vuosittain. Suunnitelman tarkistaminen on ajankohtaista myös silloin, kun tietojärjestelmässä tai työmenetelmissä tapahtuu merkittäviä muutoksia. Tietoturvasuunnitelman laatiminen kuuluu organisaation turvallisuudesta huolehtiville henkilöille sekä tietohallinnolle. Suunnitelman sisältämien yksityiskohtaisempien tietojen takia dokumentti on luottamuksellinen tai salainen.

Tietoturvasuunnitelma voi joissakin tapauksissa soveltua sellaisenaan tietoturvaohjeeksi tietojärjestelmän peruskäyttäjälle. Usein suunnitelma sisältää kuitenkin liian paljon teknisiä yksityiskohtia ja silloin vaarana on, että käyttäjä ei jaksa keskittyä noudattamaan kaikkia ohjeita ja määräyksiä. Samalla tietojärjestelmän käyttäjälle voi jäädä myös epäselväksi ohjeen tarkoitus ja merkitys juuri hänen työtehtäviään ajatellen. Peruskäyttäjälle selkeät, juuri hänen työtehtäviään koskevat ohjeistukset ja käytännönläheiset esimerkit ovat eniten hyödyksi. Tietoturvaohje kuuluu myös luottamuksellisiin tai salassa pidettäviin asiakirjoihin.

Pelkkä tietoturvallisuuden ylläpitoon tähtäävä ohjeistus ei ole yleensä riittävä. Ohjeistuksen lisäksi tarvitaan myös koulutusta ja valvontaa. Henkilökunta tulisi kouluttaa heti työsuhteen alussa tietoturvan huomioimiseen jokapäiväisissä toiminnoissa. Lisäksi tietoturvakoulutusta on hyvä järjestää säännöllisesti työsuhteen aikana, koska annetut ohjeet unohtuvat helposti. [3.]

Työntekijälle on tärkeää, että hän myös ymmärtää, miksi organisaatiossa toimitaan tiettyjen pelisääntöjen mukaan ja mikä merkitys niillä on toiminnan jatkuvuudelle. Tietoturvallisuuden toteutumista tulee tarkkailla jatkuvasti, jotta väärinkäytöksiin pystytään puuttumaan ajoissa, eikä toiminnalle aiheudu katkoksia tai suuria taloudellisia vahinkoja. [3.]

Väärinkäytösten varalle tulee organisaatiolla olla selkeä suunnitelma ja määritellyt rangaistukset tietoturvapolitiikan tai -ohjeistuksen rikkomisesta. Kurinpitomenettely laaditaan organisaation henkilöstötavoitteiden mukaan ja se on johtoryhmän hyväksymä. Kurinpitomenette-

lyllä on ehkäisevä vaikutus sellaisten henkilöiden kohdalla, joilla on tapana olla välittämättä tietoturvallisuudesta annetuista ohjeista. Menettely takaa myös oikeudenmukaisen kohtelun vakavasti ja toistuvasti turvaohjeita rikkovalle henkilölle.

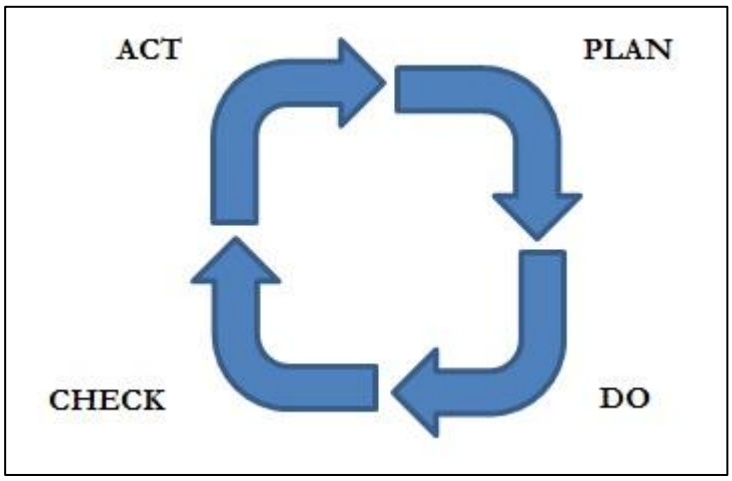
Jokaisella työntekijällä on vastuu omasta työstään ja tietoturvallisuuden huolehtimisesta omalta osaltaan. Organisaatioissa on yleensä nimettynä tietoturvallisuudesta kokonaisuudessaan vastaava henkilö, jolla on oltava riittävästi tietoa ja taitoa tietoturvallisuudesta sekä yhteyksiä ulkopuolisiin alan ammattilaisiin. Lisäksi tietoturvan vastuualueita voidaan jakaa useiden henkilöiden kesken ja isoissa organisaatioissa se on jopa välttämätöntä. [3.]

Tietoturvallisuudesta vastaavien henkilöiden tehtäviä on lueteltu taulukossa 1.

Taulukko 1. Tietoturvallisuuden ylläpidon tehtäviä [3.]

Tietoturvallisuuspäällikkö	Johtaa organisaation tietoturvallisuusasioiden kehittämistä
	Tietoturvapolitiikan määrittely ja ylläpidosta huolehtiminen
	Tietoturvallisuusmallien suunnittelu
	Perussuojaustason määrittely
	Tietoturvakoulutuksen järjestäminen
	Sisäinen tiedottaminen
	Yhteydenpito sisäisiin sidosryhmiin
	Yhteydenpito yhteistyökumppaneiden turvallisuudesta vastaaviin henkilöihin
	Yhteydet viranomaisiin tietoturvallisuusasioissa
	Alan kehityksen seuraaminen kotimaassa ja ulkomailla
	Vuosikertomuksen laatiminen turvallisuustoimiin liittyen
Asiantuntija, suunnittelija	Kehittämisprojektin päällikkönä toimiminen
	Riskianalyysin laadinta ja riskien vaikutusten arviointi
	Suojausmenetelmien ylläpito ja kehittäminen

Tietoturvallisuuden ylläpito vaatii jatkuvasti toimenpiteitä ja se muodostaa oman toiminta-prosessinsa. ISO/IEC 27001 -standardi määrittelee tietoturvallisuuden hallintajärjestelmälle (Information Security Management System, ISMS) asetetut vaatimukset. Standardin mukaan tietoturvallisuuden johtaminen ja hallinta on prosessi, jossa organisaation toimintojen ja toimintaympäristön muuttuessa myös tietoturvallisuuden hallintajärjestelmää kehitetään vastaavasti. Prosessin perustana on PDCA-malli (Plan-Do-Check-Act), (kuva 3). Mallin mukaan tietoturvallisuuden hallinta toteutetaan tietyn vaihejaon mukaisesti. PDCA-mallin vaihejako ja soveltaminen on nähtävillä taulukossa 2.



Kuva 3. PDCA-malli toiminnassa

Taulukko 2. PDCA-mallin soveltaminen

P	Hallinnan suunnittelu ja hallintajärjestelmän (ISMS) luonti (establishing)	Tietoturvapolitiikka, turvallisuuden tavoitteet, prosessit, riskianalyysi, menettely riskin toteutuessa
D	Toteutus (implementing, operating)	Hallintajärjestelmän käyttöönotto ja käyttäminen normaalissa toimintaympäristössä
C	Tarkastelu ja seuranta (reviewing, monitoring)	Tietoturvallisuuden toteutumisen mittaus Vertailu tietoturvapolitiikan määrittelyihin
A	Ylläpito ja parantaminen (maintaining, improving)	Korjaukset havaittuihin puutteisiin, uudet haasteet

Tietoturvakartoituksen avulla pystytään saamaan selville organisaation tietoturvallisuuden tila. Kartoitus tulee suorittaa säännöllisin väliajoin, ja kartoituksessa ilmenneisiin puutteisiin tulee puuttua välittömästi. Tietoturvakartoitus ei korvaa normaalia tietoturvallisuuden toteutumisen seurantaa.

3.2 Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan toimitilojen, laitteistojen ja henkilöstön suojaamista erilaisten fyysisten uhkien varalta. Organisaatiota ja sen henkilöstöä uhkaavia fyysisiä tekijöitä ovat ilkivalta, murrot, varkaudet, väkivalta, vesi- ja palovahingot ja sähkö- ja lämmitysjärjestelmien häiriöt.

Fyysisen turvallisuuden vaatimukset vaihtelevat suuresti erilaisten organisaatioiden välillä. Vaatimuksiin vaikuttavat esimerkiksi organisaation toiminnan laatu ja laajuus sekä käytetyn tietotekniikan määrä.

Tietoturvastandardin mukaan tietotekniset laitteet, joita käytetään organisaation kriittisiin toimintoihin tai arkaluonteisen tiedon käsittelyyn, sijoitetaan turva-alueelle. Tavoitteena on estää luvaton tunkeutuminen ja siitä aiheutuvat vahingot ja häiriöt. Turva-alue suojataan asianmukaisesti riittävällä lukituksella ja kulunvalvonnalla. Vesi- ja palovahinkojen minimointi on huomioitu tilojen rakenteissa ja rakennusmateriaaleissa. Turva-alue määritellään selkeästi ja suojauksen taso on riippuvainen suojattavasta aineistosta tai palvelusta.

Organisaation sisäisesti hallinnoimat tietokonelaitteet sijoitetaan omille alueilleen siten, että ulkopuoliset tai muu henkilökunta eivät pääse niitä käyttämään. Esimerkiksi palvelinhuoneen fyysisen suojauksen on oltava korkeatasoinen, eikä tiloihin saa olla pääsyä muilla kuin tietojärjestelmän ylläpitäjillä. Palvelinhuoneen sijainti ei saa olla yleisesti tiedossa. Palvelinhuoneen ilmanlaatuun ja lämpötilaan tulee kiinnittää huomiota. Liian korkea lämpötila saattaa aiheuttaa eheys- ja käytettävyysongelmia.

Turva-alue suojataan asianmukaisella kulunvalvonnalla. Tällä varmistetaan, että alueelle on pääsy vain luvallisilla henkilöillä. Alueella liikkuvien henkilöiden liikkeistä tallennetaan päiväys ja kellonaika. Työsuhteen päättyessä kulkuoikeus turva-alueelle on peruutettava välittömästi.

Palvelinhuoneissa ei yleensä ole viemäröintiä, koska viemärit saattavat tulvia ja siten aiheuttaa vesivahinkoja. Tulvimisen ehkäisemiseksi voidaan käyttää lattiakaivoja, jotka on suojattu tulvimiselta. Palvelinhuoneiden suositeltu ilmankosteus on 40–60 %. Jos ilmankostutukseen käytetään vesijohtoverkkoon kytkettyjä ilmankostuttimia, on huolehdittava myös ylimääräisen veden poistamisesta ilmankostuttimen rikkoutuessa. Ilmankostuttimet voidaan varustaa vuotoaltailla ja vesijohtoon voidaan laittaa paineventtiilin avulla toimiva automaattinen sulkumekanismi. Paineventtiilien toimivuus turvataan huoltamalla ja testaamalla ne vuosittain.

Puhtaan pöydän politiikalla tarkoitetaan sitä, että tietoaineistoja ei säilytetä jatkuvasti nähtävillä. Paperit, CD-levyt tai muut tallennusvälineet säilytetään kaapeissa, jotka saa tarvittaessa lukittua. Tietoaineisto, joka on jätetty pöydälle, vaurioituu tai tuhoutuu helpommin tulipalon tai vesivahingon seurauksena. Lisäksi vapaasti lojuva aineisto on varkaalle helppo saalis. Arkaluonteisia tietoja sisältävät asiakirjat ja tallennusvälineet tulee sijoittaa lukittuun palonkestävään kassakaappiin aina silloin, kun niitä ei tarvita. Tietojen luvatonta käyttöä voidaan estää myös lukitsemalla henkilökohtainen työasema ja työhuoneen ovi poistuttaessa huoneesta.

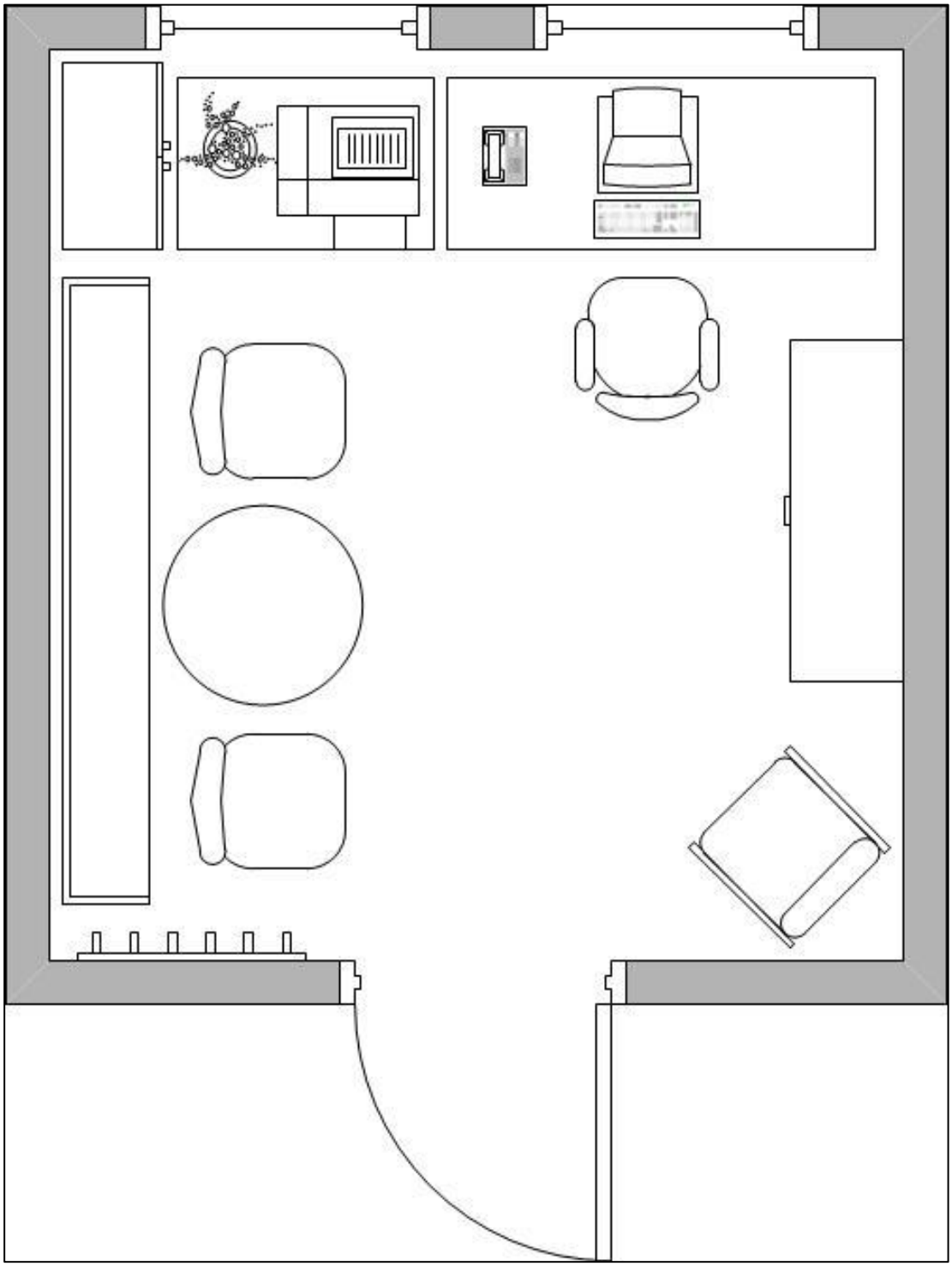
Tulipalo on vakava uhka sekä tietoaineistoille että henkilöstölle. Henkilöstöä uhkaavat myös muut vaarat, kuten väkivalta. Väkivallan uhka on todellinen ja mahdollinen hyvin monella työpaikalla. Suurimmassa vaarassa ovat asiakaspalvelussa ja vastaanotossa työskentelevät henkilöt, mutta häiriintynyt asiakas voi yllättää myös muualla.

Kuvassa 4 on nähtävillä perinteinen työhuoneen järjestys. Työntekijällä on hyvät näkymät ulos ikkunasta ja huoneessa voi ottaa vastaan vierailijoita. Huone on avara, eikä sitä ole täytetty turhilla kalusteilla. Henkilön turvallisuuden ja tietoturvan kannalta tällainen huoneen järjestys ei ole kovin hyvä.

Työntekijä istuu selkä ovelle päin, eikä siten voi välittömästi havaita huoneeseen pyrkivää tulijaa (mikäli ovea pidetään auki), jos tämä liikkuu äänettömästi. Huoneeseen pyrkivä tulija voi urkkia tietoja katselemalla niitä tietokoneen näytöltä tai valokuvaamalla. Pahimmassa tapauksessa tulija on häiriintynyt ja vaaraksi työntekijälle. Uhkaavassa tilanteessa työntekijällä ei ole mahdollisuutta paeta huoneesta ja hyökkääjällä on suora reitti työpisteelle. Ikkuna olisi ainoa pakotie kyseisestä huoneesta, mutta se ei ole kovin kätevä eikä turvallinen, jos työhuone sijaitsee rakennuksen ylemmissä kerroksissa.

Kuvan 4 kalusteiden sijoittelussa huonoa on myös tulostimen paikka. Tulostimeen unohtunut paperi on vierailijan ulottuvilla.

Työhuoneesta poistuttaessa ovi ja työasema on muistettava lukita, jotta tietoja ei joudu vääriin käsiin. Tietovuodon lisäksi huolimaton työntekijä voi joutua vaikeuksiin myös sen takia, että jokainen järjestelmän käyttäjä on yleensä vastuussa kaikista omilla tunnuksilla tehdyistä asioista. Tunnusten väärinkäyttöä on hankala todistaa ja siksi on parempi olla huolellinen. Myös laitteiden varastaminen lukitsemattomasta huoneesta on mahdollista ja ammattilaiselle riittää lyhytkin aika tavaroiden viemiseen.



Kuva 4. Perinteinen työhuoneen järjestys

Kuvassa 5 on nähtävillä hieman turvallisempi työhuone. Kalusteita on hieman enemmän kuin edellisessä esimerkissä, mikä tekee huoneesta ahtaamman. Osa kalusteista on myös erilaisia edelliseen esimerkkiin verrattuna.

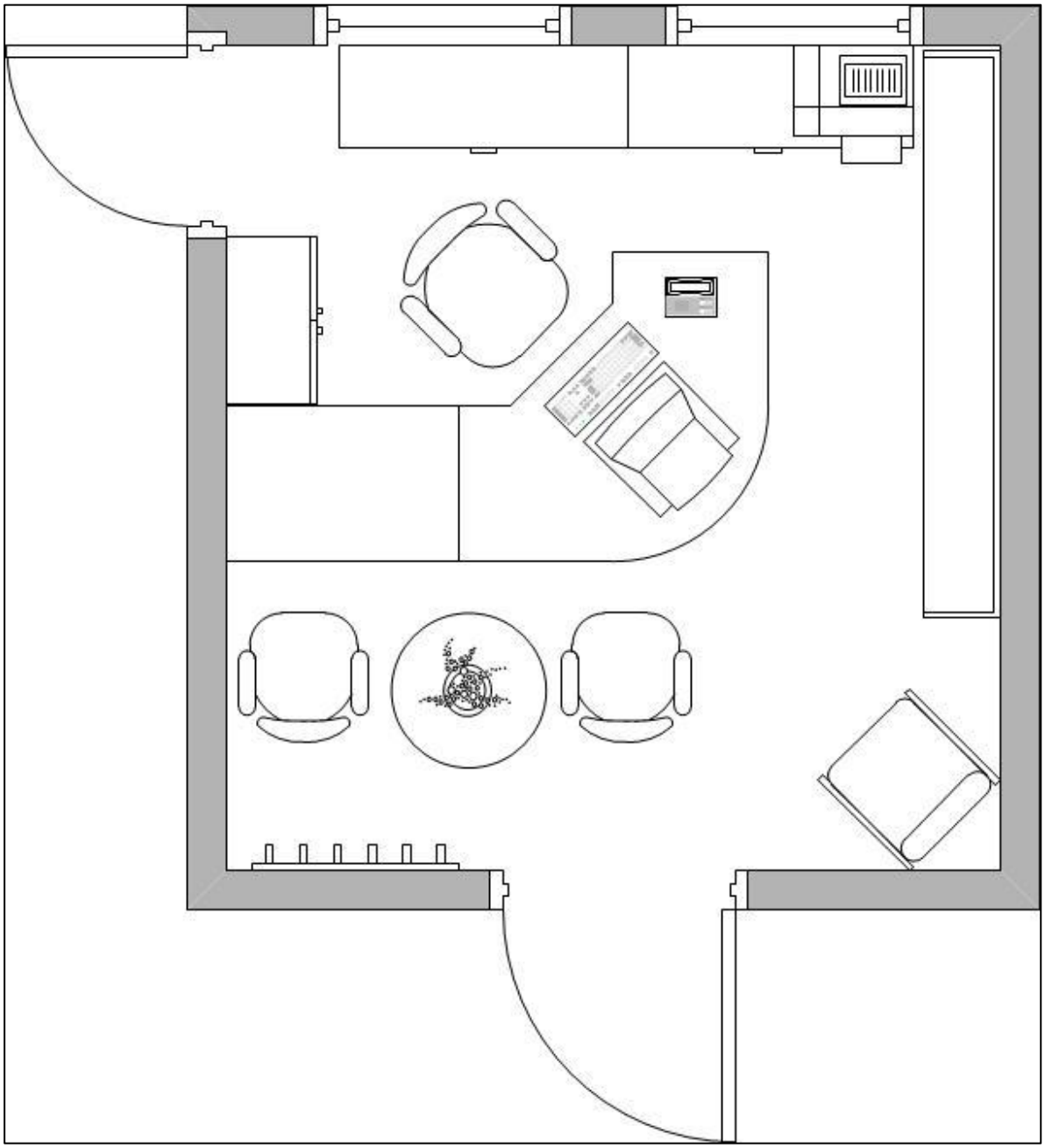
Työntekijä istuu tässä huoneessa vinoittain oveen nähden, mutta hänellä on kuitenkin hyvä näkyvyys ovelle ja huoneeseen saapuvat henkilöt on helppo havaita. Saapuvalla henkilöllä ei ole suoraa näkyvyyttä tietokoneen näytölle, joten tietojen urkkiminen ei ole mahdollista. Pieni mahdollisuus näytön tietojen urkkimiseen on ikkunan kautta. Uhkan todennäköisyys on kuitenkin melko pieni ja riippuu paljolti työhuoneen sijainnista rakennuksessa (kerrokset). Tätä uhkaa voidaan pienentää esimerkiksi sälekaihtimilla.

Lisäksi näyttöön voidaan asentaa erillinen tietoturvasuoja, jolloin sivusta näytölle katseleva näkee vain mustan ruudun. Suoja on helppo asentaa tarrakiinnitteisillä kiinnityspaloilla ja se voidaan poistaa tarvittaessa. Suojia on saatavissa sekä pöytäkoneille että kannettaville tietokoneille. [5.]

Mikäli huoneeseen tulija on vaarallinen tai erityisen hankala asiakas, on työntekijä vähän paremmassa turvassa työpöydän takana. Työntekijällä on enemmän aikaa havaita tulijan vaarallisuus, koska tulija joutuu kiertämään pöydän taakse, mikäli aikoo tehdä jotain pahaa. Tässä työhuoneessa on toinen ovi, jonka kautta työntekijä voi poistua tarvittaessa. Ovi on sijoitettu työntekijän selän taakse ja sen kautta poistuminen onnistuu hätätilanteessa nopeasti. Varauloskäyntiä ei saa tukkia ylimääräisillä kalusteilla.

Kuvassa 5 tulostin on sijoitettu kauas vierailijoille tarkoitetuista istuimista. Vierailijalla ei pitäisi olla huoneessa asiaa tuoleja pidemmälle. Jos vierailija pyrkii hakemaan tulosteita, on se ainakin helposti havaittavissa.

Työaseman ja oven lukituksesta on huolehdittava samalla tavalla kuin edellisessäkin esimerkissä huoneesta poistuttaessa. Vierailijoita ei saa jättää yksin työhuoneeseen edes lyhyeksi aikaa. Vaarana on, että pahantahtoinen vierailija asentaa tietokoneen ja näppäimistön väliin ylimääräisen laitteen (Keylogger), joka tallentaa näppäimistön painallukset ja siten saadaan selville koneelle näppäillyt käyttäjätunnukset ja salasanat. Tietokoneen sijoittelussa on syytä huomioida tämäkin seikka. Laitteen asennus onnistuu muutamassa sekunnissa.



Kuva 5. Tietoturvallisempi työhuoneen järjestys

Ilkivaltaa ja murtoja ehkäistään vartioinnilla ja rikosilmoitinjärjestelmällä. Ulkoalueita ja varsinkin sisäänkäyntejä valvotaan tallentavien kameroiden avulla. Kameroita on hyvä sijoittaa sekä ulos että sisälle. Tilat tarkistetaan iltaisin ja varmistetaan, että tiloihin ei jää ketään ulkopuolisia. Murtoilmaisimia sijoitetaan oviin ja ikkunoihin. Hälytyksen ollessa päällä rikosilmoitinjärjestelmän tulee ilmaista myös auki olevat ulko-ovet ja ikkunat. Oven sulkeutumisen saattaa estää jokin ylimääräinen esine. Varsinkin lämpimällä ilmalla joku voi avata ikkunan ja se jää vahingossa auki. Ovien ja ikkunoiden rakenteiden tulee olla vakuutusyhtiöiden määräysten mukaiset. Sisätilat varustetaan esimerkiksi liiketunnistimilla.

3.3 Henkilöturvallisuus

Henkilöturvallisuuteen liittyvissä asioissa pääasiallisena lähteenä on käytetty Juha E. Miettisen kirjaa Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan[3].

Henkilöturvallisuus on tietoturvallisuuden osa-alue, jossa tarkastellaan organisaation tietojen ja järjestelmän suojaamista ihmisten aiheuttamilta tahallisilta tai tahattomilta uhkilta. Henkilöturvallisuus on tärkeä osa-alue, koska organisaation tärkeimpiä tietoturvallisuuden varmistajia ovat siinä toimivat ihmiset. Henkilöturvallisuutta tarkasteltaessa otetaan huomioon niin organisaation oma henkilöstö kuin sen toimintaan osallisena olevat vierailijat, asiakkaat, ulkopuoliset työntekijät ja mahdolliset muut henkilöt. Henkilöturvallisuutta on syytä ajatella esimerkiksi silloin, kun organisaatioon palkataan uusi työntekijä, työtehtävät vaihtuvat tai työsuhde päättyy.

Henkilön taustatietojen tarkistaminen on yksi tärkeimmistä henkilöturvallisuuden toteutuskeinoista. Organisaation on hyvä tarkistaa ja selvittää ennen työntekijän palkkaamista tai sopimussuhteen alkamista henkilön taustatiedot. Taustatietojen tarkistamisella vältetään tilanteet, joissa työntekijä osoittautuu rikolliseksi tai muuten epäpäteväksi.

Viranomaistarkistuksesta käytetään myös nimitystä luotettavuustarkistus, ja se on lakisääteinen toimenpide. Viranomaistarkistusta pyydetään kirjallisesti tarkistuksen tekijältä eli Suojelupoliisilta. Tarkistusta voidaan pyytää tarkistettavan henkilön kirjallisella suostumuksella ja sillä selviää, onko henkilö ollut osallisena rikollisessa toiminnassa. Kenen tahansa tietoja ei voida tarkistaa. Tarkistuspyynnön perusteena on oltava valtion turvallisuuden kannalta oleellinen asia tai huomattava taloudellinen intressi.

Työhistorian tarkistamisella varmistetaan työtodistusten aitous ja se että henkilö todellakin on ollut kyseisten organisaatioiden palveluksessa mainittuina aikoina. Työhistoria on helppo selvittää ottamalla yhteyttä aiempiin tärkeimpiin työnantajiin joko puhelimitse tai sähköpostitse. Kaikkia edellisiä työnantajia ei ole tarpeellista käydä läpi. Mikäli työhistoriassa on epäselvyyksiä, on ne selvitettävä huolellisesti ennen henkilön palkkaamista.

Viime aikoina on ilmennyt muutamissa ammateissa, mm. lääkäri ja opettaja, väärinkäytöksiä. Palvelukseen otetulla henkilöllä on ollut väärennetty tutkintotodistus ja siten hän ei ole ollut pätevä toimimaan ammatissa. Koulutustaustan tarkistuksella varmistetaan, että henkilön esittämät todistukset koulutuksesta ovat aitoja. Koulutustausta tarkistetaan todistuksissa mainituista oppilaitoksista. Pelkän koulussa läsnäolon lisäksi on hyvä varmistaa myös opintojen laajuus.

Maksuhäiriöiden ja luottotietojen tarkistaminen tulee kysymykseen silloin, kun palkattava henkilö joutuu olemaan tekemisissä organisaation rahaliikenteen kanssa joko suoraan tai välillisesti.

Joissakin tapauksissa on tarpeellista tarkistaa työnhakijan kytkökset muihin organisaatioihin. Tietoturvallisuusuhka saattaa syntyä esimerkiksi tilanteessa, jossa hakija on kilpailevan yrityksen hallintoelimen jäsen. Tiedot henkilön yrityskytköksistä löytyvät tavallisesti kaupparekisteristä.

Työnhakijan mainitsemat mahdolliset suosittelijat ovat hyvä ja nopea tapa saada lisätietoja henkilöstä, sillä edellytyksellä, että suosittelijaan voidaan luottaa. Suosittelijoiden puute voi toisaalta olla merkki ongelmista taustatiedoissa.

Internetistä löytyy paljon tietoja henkilöistä, mutta löydöksiin kannattaa suhtautua varauksella. Internet sisältää paljon virheellistä ja väärennettyä tietoa, ja se ei siten ole luotettava keino tarkistaa työnhakijan taustatietoja.

Organisaatioiden keskeiset salassapitosopimukset ja yksittäisten henkilöiden allekirjoittamat salassapitosopimukset ovat perusta henkilöturvallisuuden toteuttamiselle sopimusten avulla. Tällaisten sopimusten muoto on yleensä sellainen, että asiakirja on oikeudellisesti sitova ja voimassa joko määräajan tai toistaiseksi. Salassapitosopimus on laadittava huolellisesti ja työntekijän on tutustuttava sopimuksen sisältöön ja ehtoihin perusteellisesti ennen allekirjoittamista. Salassapitosopimus voi olla joko erillinen asiakirja, kun kyseessä on organisaation

ulkopuolinen henkilö, tai se voi sisältyä työsopimukseen vakituisen tai määräaikaisen henkilön kohdalla. Kahden organisaation välisessä sopimuksessa kumpikin osapuoli sitoutuu noudattamaan tiettyjä menettelytapoja tietojen suojaamiseksi tietojen luovuttamisen tai vastaanottamisen yhteydessä. Salassapitosopimuksessa on määriteltynä sanktiot mahdollisten sopimusrikkomusten yhteydessä.

Työ- tai sopimussuhteen päättymiseen liittyy monta muistettavaa seikkaa. Työntekijällä on muistissaan paljon tietoa ja niitä ei voida sieltä pyyhkiä pois, mutta kaikki työnantajan omaisuutta olevat tallennus- ja työvälineet sekä tietoaineisto voidaan pyytää takaisin. Tämän lisäksi työntekijän käyttöoikeus tietojärjestelmään poistetaan. Jos henkilöllä on hallussaan sellaista tietoa, mitä hän ei saa edes vahingossa ottaa mukaansa, on käyttöoikeuksia poistettava jo silloin kun työsuhteen päättyminen on tiedossa. Työntekijä velvoitetaan palauttamaan hallussaan olevat avaimet ja kulkunapit välittömästi työsuhteen päättyessä. Avainten luovutuksesta palautuksesta on hyvä pitää tarkkaa kirjanpitoa.

Jos poislähtevällä työntekijällä on ollut oikeus käyttää organisaation varoja, on tämä oikeuden poistaminen yksi tärkeimmistä toimenpiteistä. Tässä yhteydessä on muistettava perua myös kaikki luottokortit, valtakirjat ja suoraan tietojärjestelmällä käytettävät rahankäyttöoikeudet.

Lähtevän henkilön työtehtävät siirretään muille työntekijöille ja asiasta ilmoitetaan kaikille asianosaisille. Tiedottamisella varmistetaan, että lähtevä henkilö ei saa tietoonsa arkaluonteisia tietoja työsuhteen päätyttyä. Tiedottaminen kohdistuu muihin työntekijöihin, ulkopuolisiin yhteistyökumppaneihin ja asiakkaisiin.

Työmatkoihin liittyy paljon tietoturvaan kohdistuvia riskejä ja niihin varautumiseksi on organisaatiolla oltava laadittuna erillinen ohjeistus. Oman haasteensa luovat vieraisiin kulttuureihin kohdistuvat matkat, jolloin on huomioitava paikalliset käytöstavat ja yleinen tilanne kohteessa.

Yleisiä työmatkojen turvallisuusriskejä ovat mm. laiterikko ja -varkaus, tietojen katoaminen tai niiden joutuminen vääriin käsiin, matkustusasiakirjojen tai maksuvälineiden häviäminen. Kaikki ylimääräinen, mitä ei välttämättä tarvita, on jätettävä pois matkasta. Muuttuneista matkasuunnitelmista on ilmoitettava heti työpaikalle.

Matkan aikana tietoaineistoa pidetään silmällä, ja se laitetaan yöksi talteen luotettavaan säilytyspaikkaan, kuten hotellin kassakaappiin tai tallelokeroon. Hotellin henkilökunnalla (esim.

siivoojat) on pääsy hotellihuoneisiin ja he eivät välttämättä ymmärrä tietoaineiston arvoa ja saattavat pahimmassa tapauksessa hävittää asiakirjat tai saattaa ne vääriin käsiin.

Julkisilla paikoilla on vaarana joutua salakuuntelun uhriksi. Julkisilla paikoilla tai julkisissa liikennevälineissä täytyy kiinnittää huomiota ympäristöön, jos on pakko puhua työasioista ja ne ovat arkaluontoista tietoa. Lentokoneessa tietojen urkkijan on helppo saada haltuunsa tietoja, jos tietokonetta käytetään lennon aikana työtarkoituksiin.

Työkäyttöön tarkoitettuja laitteita ei saa luovuttaa kenenkään ulkopuolisen käyttöön matkan aikana. Laitteistoissa on oltava asennettuna ja käytössä luotettava turvaohjelmisto, pääsynvalvonta ja tietojen salaus. Tietokoneen tai puhelimen rikkoutuessa otetaan yhteys oman organisaation mikrotukeen ja kysytään sieltä ohjeita tilanteen korjaamiseksi.

Organisaation tietotekniset palvelut ovat yleensä monipuolisia ja niiden ylläpitoon tarvitaan ammattitaitoinen henkilökunta. Vähänkään suuremmassa organisaatiossa yksi henkilö ei pysty vastaamaan kaikista toiminnoista. Vastuualueita tulee jakaa tasapuolisesti useammalle henkilölle. Vastuualueiden jaon yhteydessä tulee huolehtia myös varahenkilöjärjestelmästä. Palveluiden saatavuus on varmistettava vastuussa olevan henkilön sairastuessa ja lomien aikana.

3.4 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus kuuluu organisaation tietohallinnon vastuualueeseen ja käsittää kaikki tietokoneiden ohjelmistoihin liittyvät asiat, mm. lisenssien ja ohjelmistoversioiden hallinta. Uusia ohjelmistoja käyttöönotettaessa on tärkeää varmistua, että uudet sovellukset ovat sopivia suunniteltuun käyttötarkoitukseen sekä yhteensopivia muiden ohjelmistojen kanssa. Lisäksi ohjelmien on oltava toiminnaltaan luotettavia ja virheettömiä. [3.]

Käyttöjärjestelmien ja kaikkien muidenkin ohjelmistojen päivittäminen on tärkeää. Ohjelmat ovat hyvin harvoin täysin virheettömiä, ja siksi niihin joudutaan tekemään jatkuvasti korjauksia. Ohjelmistojen valmistajat julkaisevat korjauksia ilmenneisiin toimintaongelmiin ja tietoturva-aukkoihin. Päivitykset saattavat aiheuttaa muutoksia ohjelman toimintaan tai olla itsessään viallisia, joten järjestelmän toimivuuden kannalta on oleellista testata myös päivitysten toimivuus, ennen niiden käyttöönottoa.

Työasema on suojattava viruksilta ja muilta haittaohjelmilta (malware) virustorjuntaohjelmalla. Haittaohjelmalla tarkoitetaan kaikkia niitä ohjelmia (virus, mato, Troijan hevonen), jotka pyrkivät asentumaan koneelle salaa ja tuottavat tietokoneelle tai koko järjestelmälle vahinkoa. Haittaohjelma voi esimerkiksi muuttaa tai tuhota kokonaan tietojärjestelmään tallennettuja tietoja. Työasema on alttiina saastumiselle, mikäli sitä käytetään muualta tulleen tiedon käsittelyyn tai se on kytkettynä verkkoon. Erityisesti käyttöjärjestelmän tietoturva-aukkoja käyttävät hyväkseen verkkomadot, jotka levittävät itseään muihin verkossa oleviin koneisiin, heti järjestelmään päästyään. Tätä uhkaa voidaan torjua käyttöjärjestelmän päivittämisellä ja käyttäjien käyttöoikeuksien rajoittamisella. [6.]

Virustorjuntaohjelma käyttää kahta eri tekniikkaa työaseman suojauksessa, manuaalista ja käytönaikaista tarkistusta. Manuaalinen tarkistus yksistään ei ole enää nykyisissä järjestelmissä riittävä, koska se vaatii aina käyttäjän toimenpiteitä. Manuaalinen tarkistus tarvitsee joko ajastuksen tai käyttäjän aktivoinnin. Käytönaikainen tarkistus toimii taustalla ja tarkkailee koko ajan koneella käsiteltäviä tietoja. Ohjelmassa voidaan erikseen määritellä kohteet, jotka tarkistettaan aina tai jätetään tarkistamatta.

Virus- ja haittaohjelmien torjunta perustuu siihen, että torjuntaohjelma vertailee tiedostoja tunnistetietokantaan. Uusia viruksia tehtaillaan jatkuvasti ja torjuntasovellus ei pysty tunnistamaan niitä, jos tunnistetietokantaa ei ole päivitetty säännöllisesti. Päivitys tapahtuu yleensä automaattisesti ja uusia virustietokantoja voi olla saatavissa useita kertoja päivässä.

Tietojärjestelmän turvallisuuden kannalta turvaohjelman toiminta ongelmatilanteessa on määriteltävä siten, että käyttäjän ei tarvitse tehdä valintaa jatkotoimenpiteestä. Järjestelmä voidaan asettaa puhdistamaan saastunut tiedosto automaattisesti. Työasemille tulevat tietoturvahälytykset on myös saatava tietoturvallisuudesta vastaavan henkilön tietoon.

Virustorjunta voi joskus pettää, ja silloin järjestelmään saattaa päästä virus tai muu haitallinen ohjelma. Tietojärjestelmän käyttäjillä on suuri vastuu tällaisissa tilanteissa. Käyttäjien tulee raportoida välittömästi atk-tuelle, mikäli he havaitsevat minkä tahansa ohjelman toiminnassa jotain tavallisuudesta poikkeavaa. Käyttäjiä ohjeistetaan kiinnittämään huomiota näytölle tuleviin ilmoituksiin ja muihin outoihin oireisiin. Kaikki viestit on syytä kirjata muistiin. Ongelmatilanteessa tietokoneen käyttö keskeytetään ja kone eristetään verkosta, mikäli mahdollista. Tallennusvälineitä ei saa siirtää muihin koneisiin.

Yksi ohjelmistoturvallisuuden tärkeimmistä suojausmenetelmistä on ohjelmiston pääsynvalvonta. Tällä pyritään estämään asiattomien käyttäjien pääsy tietojärjestelmään. Ohjelmistojen kohdalla pääsynvalvonta toteutetaan yleensä kysymällä ohjelmiston käyttöä yrittävältä käyttäjältä käyttäjätunnusta ja salasanaa. Jos käyttäjä ei tiedä oikeita tunnuksia, on käyttö estettävä joko kokonaan tai osittain. [3.]

Monet ohjelmat tallentavat toimintaansa liittyviä lokitietoja, joita voidaan tarvittaessa tarkastella. Yleisiä tallennettavia tietoja ovat esimerkiksi käyttäjätunnus, kirjautumisen ajankohta ja sen kesto. Tapahtumatiedoista on apua silloin, kun järjestelmässä tapahtuu jokin virhetilanne tai kyseessä on väärinkäyttötapaus. [3.]

Yksi yleisimmin käytetyistä perussuojaustekniikoista on ohjelmien ja tietojen varmuuskopiointi. Varmuuskopioinnin avulla varmistetaan, että organisaatiolla on ajantasaiset kopiot, jos ohjelmat tai niiden sisältämät tiedot vaurioituvat tai tuhoutuvat. Varmuuskopiointi järjestetään yleensä toimivaksi automaattisesti palvelimilla, kun tiedot tallennetaan verkkoasemalle. Jos käyttäjä tallentaa työnsä muulle tallennusvälineelle, on hänen huolehdittava varmuuskopioinnista itse manuaalisesti. Varmuuskopiointi on suoritettava säännöllisesti, esimerkiksi iltaisin, päivän aikana muuttuneiden tietojen osalta, ja viikoittain kaikkien tietojen osalta. Varmuuskopiot säilytetään erillään varsinaisista tiedoista sekä ohjelmista, jotta ne säilyvät vahingoittumattomina onnettomuustilanteissa. Tietojen palautusta varmuuskopioista on myös testattava säännöllisesti. Varmuuskopioilla ja niiden ottamisella ei ole mitään merkitystä, jos palauttaminen ei onnistukaan tarvittaessa. [3.]

Taulukossa 3 on mainittuna erilaisia varmistustapoja.

Taulukko 3. Erilaisia varmistustapoja [2.].

Varmistustavat	
Varmistettava asia	**Palautusskenaario**
Käyttöjärjestelmä ja asetukset	Käyttöjärjestelmään tehtävien muutosten yhteydessä (päivitykset, laiteasennus, uudet ohjelmat)
Käyttöjärjestelmä ja asetukset, muut ohjelmistot ja niiden asetukset	Edellisen lisäksi, jos ohjelmistopäivityksessä ilmenee ongelmia
Järjestelmän sisältämät tiedot	Tiedot voidaan palauttaa, jos ne ovat tuhoutuneet tai muuttuneet
Koko palvelimen varmistaminen (käyttöjärjestelmä, ohjelmat, data)	Palvelimen palauttaminen ennalleen
Yhden sovelluksen tiedot	Sovelluskohtainen palauttaminen tai tietojen siirtäminen toiseen järjestelmään

Tietokoneohjelmiin liittyy paljon dokumentteja, joissa on kuvattuna ohjelman rakenne ja toiminta sekä käyttöohjeet. Ohjelmistodokumentaatio on siinä mielessä tärkeä, että virhetilanteessa voi olla hankalaa selvittää virheen laatu ja korjaustoimenpiteet, ilman kunnollista ohjeistusta. Organisaatiolle dokumentaatiosta on eniten hyötyä silloin, kun se on tarpeeksi kattava ja ajan tasalla. [3.]

Organisaation käytössä olevat ohjelmistot on hankittava laillisesti ja rekisteröitävä, jotta organisaatiota ei voida syyttää laittomien ohjelmien käytöstä. Ohjelmistot hankitaan vain viralllisten ja luotettavien toimittajien kautta. Ohjelmistolisenssien hallinnalla varmistetaan lisenssien ajantasaisuus ja häiriötön toiminta. [3.]

3.5 Laitteistoturvallisuus

Laitteistoturvallisuus liittyy osittain myös fyysiseen turvallisuuteen, mutta siihen sisältyy myös muita seikkoja, jotka taas eivät kuulu fyysisen turvallisuuden piiriin. Laitteistoturvallisuus on käsitteenä hyvin laaja ja siihen voidaan sisällyttää kaikki organisaation toiminnassa käytettävät tekniset laitteet. Laitteistoturvallisuuden tavoitteena on omaisuuden häviämisen ja vahingoittumisen estäminen sekä organisaation toimintojen jatkuvuus.

Kouluympäristössä ATK-luokissa tulee olla kameravalvonta ehkäisemässä omaisuuden häviämistä tai vahingoittumista. Muita mahdollisia laitteisiin kohdistuvia riskejä ovat: tulipalo, savu, vesi, tärinä, kemialliset vaikutukset, pöly, sähköhäiriö ja sähkömagneettinen säteily. Kemiallisia vaikutuksia estetään esimerkiksi kieltämällä syöminen ja juominen tietokoneluokissa. Toimintojen kannalta kriittisten laitteiden yhteydessä on kannattavaa käyttää varavirtalähdettä eli UPS-laitetta. UPS mahdollistaa järjestelmän hallitun alasajon virransyötön katketessa. Varavirtalähde on testattava säännöllisesti laitteen valmistajan ohjeiden mukaisesti.

Kaikkiin tiloihin tulee asentaa asianmukaiset varoittimet ilmaisemaan lämpötilan kohoaminen tai savu. Alkusammutusvälineet ja muut turvalaitteet tulee tarkistaa valmistajan ohjeiden mukaisesti. Alkusammutusvälineet on pidettävä helposti saatavilla ja henkilökunta tulee kouluttaa niitä käyttämään. Vesi ei sovellu tietoteknisten laitteiden palossa sammuttamiseen. [3.]

Tietotekniset laitteet vaativat säännöllistä huoltoa, jotta niiden jatkuva käytettävyys ja tiedon eheys varmistuvat. Laitteiden huollossa noudatetaan valmistajan antamia ohjeita koskien huoltoväliä ja muita määräyksiä. Laitteiden korjauksesta vastaavat henkilöt, jotka ovat siihen päteviä. Kaikista laitteissa ilmenneistä vioista tai vikaepäilyistä on pidettävä kirjaa. [4] Laitteiden hankinnan yhteydessä on mahdollista laatia ylläpito- ja huoltosopimus, jolla varmistetaan laitteiston häiriötön toiminta. Sopimuksessa määritellään tarkasti siihen sisältyvät asiat ja esimerkiksi huoltopalveluiden saatavuuden nopeus. Myös varaosien saanti on hyvä varmistaa laitteiden hankinnan yhteydessä sopimuksella. [3]

Laitteiden pääsynvalvonta on yksi tärkeimmistä laitteistoturvallisuuden menetelmistä. Pääsynvalvonnalla estetään laitteen luvaton käyttö joko suoraan laitteeseen kirjautumalla tai etäyhteyden avulla. Laitetasolla pääsynvalvonta toteutetaan tavallisesti kysymällä käyttöön

oikeuttavaa käyttäjätunnusta ja salasanaa. Ilman oikeita tunnuksia konetta tai organisaation tietoverkkoa ei pysty käyttämään. [3.]

Useimmissa tietoteknisissä laitteissa on jokin menetelmä, jolla kerätään lokitietoja laitteen käytöstä. Väärinkäytön tai laitteen vioittumisen yhteydessä voidaan tapahtumatietojen avulla paikallistaa tai selvittää poikkeustapauksen aiheuttaja. Tavallisimmin tallennetaan tiedot sisään kirjautumisista laitteelle sekä siihen mahdollisesti syötetyt käskyt tai komennot. [3.]

Organisaation kaikki toiminnot eivät ole yhtä kriittisiä. Toiminnoissa mukana olevia laitteita voidaan jaotella niiden kriittisyyden mukaan. Laitteita ei ole yleensä tarpeellista varmentaa, mutta joissakin erityisissä tilanteissa se on ainoa tapa varmistua toiminnan jatkuvuudesta. Esimerkiksi palvelin voi olla tällainen kriittinen laite. Laitteen varmentaminen hoidetaan hankkimalla toinen vastaava laite (kahdentaminen), joka hoitaa tarvittaessa alkuperäisen laitteen tehtävät. Varmentava laite voi toimia varsinaisen laitteen kanssa koko ajan tai se voi olla käyttövalmiudessa ja voidaan ottaa nopeasti käyttöön korvaamaan vioittunut laite. [3.]

Organisaation laitteistosta pidetään rekisteriä, josta selviää mm. laitteiden sarjanumerot, malli ja sijoituspaikka. Laitteistorekisterin lisäksi kannattaa laitteistosta olla olemassa dokumentaatio helpottamaan ongelmatilanteiden selvittelyä laitteen rikkoontuessa tai toimiessa muuten virheellisesti. Dokumentaatiossa tulee olla kuvaus laitteiden teknisistä rakenteista sekä yksityiskohtaiset käyttöohjeet. Dokumentaation on oltava helposti saatavissa joko kirjallisena tai sähköisenä versiona. [3.]

Vanhentuneet ja tarpeettomat laitteet on poistettava käytöstä siten, että organisaation luottamukselliset ja arkaluonteiset tiedot eivät paljastu ulkopuolisille. Laitteiden käytöstä poistamisen yhteydessä on huomioitava kaikki sellaiset laitteet, jotka jollain tavalla tallentavat tietoa (muistikortit, tulostimet, puhelimet, muistitikut). Kiintolevyillä huomioitavaa on arkaluonteinen tieto sekä tekijänoikeuksien piiriin kuuluvat tiedot.

3.6 Tietoaineiston turvallisuus

Tietoaineistoturvallisuus käsittää erilaisissa muodoissa tallennettuja jokapäiväisessä toiminnassa tarvittavia tietoja sekä niiden suojaamiseen liittyviä seikkoja. Tietoaineistoturvallisuuden toteutuksen perustana on tietojen turvaluokittelu. Turvaluokitusjärjestelmässä kuvataan,

minkätyyppistä tietoa organisaatiossa käsitellään, miten tärkeitä tiedot ovat toisiinsa nähden, miten turvaluokitellut tiedot merkitään ja miten luokiteltuja tietoja käytetään tiedon elinkaaren eri vaiheissa [2]. Valtionhallinnossa tietojen luokittelussa käytetään lainsäädännön määrittelemää luokitusta [7]. Muissa organisaatioissa voidaan käyttää itse luotua ja omaan käyttöön soveltuvaa luokittelua.

Taulukossa 4 on nähtävillä useimpien organisaatioiden käyttöön soveltuva tiedon luokittelu.

Taulukko 4. Tietojen luottamuksellisuuden luokittelu [2.]

TIEDON LUOKITTELU		
Luokka	**Kriteerit**	**Esimerkit**
Julkinen	Sisältää tietoa, joka voidaan julkaista vapaasti. Ei sisällä organisaation toimintaa tai julkisuuskuvaa vahingoittavaa tietoa.	• markkinointimateriaali • lehdistötiedotteet • julkisten rekistereiden tiedot
Sisäinen	Tieto, joka on organisaation ja / tai sidosryhmien sisäiseen käyttöön tarkoitettua.	• tiedotteet henkilöstölle • rahtikirjat • sisäiset puhelinluettelot
Luottamuksellinen	Organisaation ja sen sidosryhmien rajoitettuun käyttöön tarkoitettua tietoa. Tietoja, joiden joutuminen vääriin käsiin aiheuttaa merkittäviä taloudellisia vahinkoja tai niiden julkaiseminen vahingoittaa organisaation mainetta.	• sopimukset asiakkaiden ja tavarantoimittajien kanssa • tarjoukset • taloushallinnon dokumentit
Salainen	Tietoa, joka on tarkoitettu organisaation sisäiseen käyttöön ja on tarkoin rajoitettu. Sisältää tietoja, joiden vuotamisella on erittäin vakavia taloudellisia vaikutuksia tai haittaa organisaation julkisuuskuvalle. Tietojen vuotaminen vaarantaa myös organisaation toiminnan jatkuvuuden. Salassapito perustuu joko lainsäädäntöön tai organisaation strategisiin linjauksiin.	• liiketoiminnan ja tuotteiden kehittämiseen liittyvät dokumentit • henkilötiedot • tietoturvallisuuden tekninen toteutus

Myös tietojen saatavuus voidaan luokitella niiden kriittisyyden mukaan. Ei-kriittisen tiedon tuhoutumisella tai sen saannin estymisellä ei ole suurta merkitystä organisaation toiminnalle. Ei-kriittinen tieto ei aiheuta tuhoutuessaan rahallista tai imagollista vahinkoa.

Kriittisen tiedon tuhoutuminen aiheuttaa merkittävää vahinkoa organisaatiolle ja sen toiminnalle. Lyhytaikaisella saannin estymisellä on vähäisiä tai kohtalaisia taloudellisia vaikutuksia ja imagovahinkoja. Pitkäaikaisella saatavuuden estymisellä vahingot ovat merkittäviä.

Erittäin kriittisen tiedon tuhoutumisella katsotaan olevan vakavia vaikutuksia organisaation toiminnan jatkuvuudelle. Lyhytaikaisella saatavuuden estymisellä on merkittäviä taloudellisia vaikutuksia ja huomattavia vaikutuksia imagoon. Erittäin kriittisen tiedon tallentamiseen ja säilyttämiseen organisaatiolla on lainsäädäntöön perustuva velvollisuus.

Eheyden osalta käytetään luokittelua, jossa arvioidaan tiedon virheettömyyttä. Virhesietoisessa materiaalissa voi esiintyä asia- tai merkkivirheitä ilman, että ne aiheuttavat suuria vaikutuksia organisaation toiminnalle.

Vähävirheinen tieto saattaa sisältää hieman merkkivirheitä, mutta niillä ei ole suurta merkitystä toiminnalle. Asiavirheillä katsotaan kuitenkin olevan olennainen vaikutus organisaation toiminnalle ja ne voivat aiheuttaa huomattavia kustannuksia ja vahinkoa imagolle. Virheellisen tiedon korjaamisesta jälkikäteen ei aiheudu oikeudellisia seuraamuksia.

Virheettömäksi luokitellussa tiedossa ei saa olla merkki- eikä asiavirheitä lainkaan. Virheellinen tieto aiheuttaa vakavia taloudellisia ja imagollisia seuraamuksia. Virheellisen tiedon korjaaminen jälkikäteen aiheuttaa oikeudellisia seuraamuksia.

Tärkeiden tietojen joutuminen vääriin käsiin voi aiheuttaa organisaatiolle joko huomattavia taloudellisia seuraamuksia tai oikeudellisia toimenpiteitä. Tietojen väärinkäytön ehkäisemiseksi on erityisen tärkeää, että jokainen organisaatiossa työskentelevä henkilö ymmärtää tiedon arvon, osaa käsitellä sitä oikein ja hallitsee sen suojauksen jokaisessa tiedon elinkaaren vaiheessa. [3.]

Organisaatiossa tietojen säilyttäminen toteutetaan tietoturvapolitiikan määritysten mukaisesti. Dokumentit ja tallennusvälineet säilytetään tarvittaessa lukollisissa kaapeissa tai tarvittaessa paloturvallisissa tiloissa. Aiemmin mainittua puhtaan pöydän politiikkaa on hyvä noudattaa tietoaineiston turvallisuudesta huolehdittaessa.

Tiedon säilyttäminen on tärkeää, mutta on myös muistettava, että tieto on hävitettävä luotettavasti sitten, kun sitä ei enää tarvita. Työntekijöiden ohjeistuksessa on oltava mainittuna oikeaoppinen dokumenttien ja tallennusvälineiden hävittäminen. Arkaluontoista tietoa sisältävät paperitulosteet tuhotaan silppurilla tai ne laitetaan lukittuun roskalaatikkoon, jonka tyhjentämisestä ja dokumenttien tuhoamisesta huolehtii luotettava taho. [6.]

Käytöstä poistetun tietokoneen kiintolevy saattaa sisältää hävitettävää tietoa. Kukaan ei pysty muistamaan, mitä tietoa levylle on joskus tallennettu. Kiintolevyn ongelmana on myös se, että pieneen tilaan mahtuu suuri määrä tietoa. Kiintolevyn formatointikaan ei poista tietoja, ja ne voivat olla palautettavissa jälkikäteen. Formatoinnilla tuhotaan ainoastaan kiintolevyllä olevien tiedostojen sijainnista kertova kirjanpito, mutta itse tiedot ovat tallella. Päällekirjoituksella tai tiedoston silppuamisella (shred) voidaan estää alkuperäisen tiedon palauttaminen. Tiedostojen silppuamista varten on olemassa lukuisia apuohjelmia. Kiintolevy on täysin käyttökelpoinen päällekirjoituksen ja alkuperäisten tiedostojen tuhoamisen jälkeen. Ilma ja pöly tuhoavat kiintolevyn pinnan siten, että kotikonstein tietoja ei pysty enää lukemaan. Täydellisen levyn mitätöinnin voi toteuttaa tuhoamalla kiintolevyn mekaanisesti. Tuhoaminen tapahtuu aukaisemalla kiintolevyn kotelo, irrottamalla elektroniikkaosan ja naarmuttamalla levypinta. Demagnetointi vastaa kiintolevyn fyysistä tuhoamista, jolloin levyn sisältö ei ole käytettävissä edes formatoimalla se uudestaan. Demagnetointiin käytettävät laitteet ovat kalliita ja siksi laitteita on käytössä vain suurimmissa yrityksissä ja esimerkiksi puolustusvoimissa, missä käsiteltävä tieto on erityisen luottamuksellista. Kiintolevyjen tyhjentäminen ja tuhoaminen on mahdollista hoitaa ostopalveluna. [6.]

Muistikortit ja -tikut tyhjennetään ennen kuin ne heitetään pois tai luovutetaan toiselle henkilölle. Tietokoneen kannalta tällaiset tallennusvälineet ovat tavallisia kiintolevyjä. Vaikka niiden sisältämä tieto olisi poistettu tietokoneessa tai digitaalikamerassa, on se kuitenkin palautettavissa. Tietojen palauttamiseen vaikuttaa myös tiedostojen pirstoutuneisuus samoin kuin kiintolevyn yhteydessä. Palautus onnistuu sitä helpommin, mitä vähemmän pirstoutumista on tapahtunut. Pienen koon takia muistikortit ja -tikut on helppo tuhota fyysisesti, mikäli se on aiheellista. [6] Pienikokoisten tallennusvälineiden yhteydessä kannattaa harkita tarkkaan, onko niihin tarpeellista tallentaa kovin arkaluontoista tietoa. Pienen koon takia tallennusväline unohtuu helposti väärään paikkaan tai häviää kokonaan.

Myös kiinteää muistia sisältävät laitteet, kuten älypuhelimet, on tyhjennettävä huolellisesti. Mikäli puhelimessa ei voida käyttää mitään pyyhintäohjelmaa, kannattaa muisti täyttää roskatiedostoilla muutamaan kertaan. [6.]

Puhelimen SIM-kortti sisältää muistia, johon tallennetaan yhteystiedot ja tekstiviestit. Tarpeeton kortti tyhjennetään puhelimen omilla toiminnoilla ennen sen hylkäämistä. SIM-kortin tiedot ovat palautettavissa erikoislaitteilla, joita on esimerkiksi poliisin käytössä. [6.]

CD- ja DVD-levyjä käytetään nykyään paljon ja niissä olevaa tietoa ei voida kaikista levyistä (cd-r ja dvd-r) poistaa tai päällekirjoittaa. Levyt on kuitenkin helppo tuhota mekaanisesti esimerkiksi siihen tarkoitukseen varustellulla paperisilppurilla. Cd-rw- ja dvd-rw-levyt voidaan tyhjentää ja niihin voidaan tallentaa uutta tietoa. Mikroaaltouuni tuhoaa levyt nopeasti käyttökelvottomiksi, mutta toimenpide irrottaa levyn pinnasta terveydelle haitallisia kemikaaleja, joten sitä keinoa ei ole turvallista käyttää. Myös mikroaaltouuni kärsii levyjen käsittelystä. [6.]

3.7 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus käsittää erilaiset tiedonsiirtoratkaisut, kuten lähi- ja laajaverkkoyhteydet sekä muut viestintäjärjestelmät. Tietoliikenneturvallisuuden tavoitteena on turvata organisaation tietoliikenteen häiriötön toiminta ja tietojen suojaus tiedonsiirron, varastoinnin ja käsittelyn aikana yleisessä tai organisaation suljetussa verkossa. Erityisesti pyritään siihen, että siirrettävä tieto ei joudu ulkopuolisten käsiin ja tietoliikenne toimii luotettavasti siirron jokaisessa vaiheessa. [3.]

Tietoliikenteen toimivuus ja turvallisuus vaatii huolellista suunnittelua. Suunnittelussa on otettava huomioon tahallisten tietomurtojen ja palvelunestohyökkäysten torjumisen lisäksi myös verkon ja kapasiteetin riittävyys. Satunnaisten ruuhkien aikana on tärkeiden tietojen käyttämisen oltava mahdollista.

Tietoliikenteelle tyypillisiä uhkia ovat yhteyskatko, tietovuoto, verkon käytön estyminen, luvaton käyttö ja eheysvirheet. Yhteyskatkon aiheuttajana voi olla kaapelirikko tai jonkin yhteyden muodostamiseen käytettävän laitteen rikkoontuminen tai altistuminen vedelle tai tuli-

palolle. Tietoliikennelaitteistojen säännöllisestä huollosta on huolehdittava laitteistotoimittajan ohjeiden mukaisesti. [8.]

Tietovuoto voi olla mahdollista silloin, jos verkkoa salakuunnellaan tai jos tietoja kopioidaan välivarastoista (puskurit, lokit). Tietovuotojen ehkäisemiseksi kaapelit ja liittimet suojataan fyysisesti luvattomalta käytöltä. Käyttämättömät liitinrasiat jätetään kytkemättä ristikytkentään ja käyttämättömät portit aktiivilaitteista suljetaan. [8.]

Vika laitteiston ohjelmistossa tai itse laitteessa voi estää tietoliikenteen kokonaan tai hidastaa sitä. Jokin verkon osa voi hidastua liian suuren kuormituksen takia. Verkon turvallisuutta voidaan parantaa käyttämällä valokuitukaapelia. Valokuitukaapeliin kytkeytyminen luvattomasti on hankalaa ja tiedonsiirtokapasiteetti on suuri. Verkon luvaton käyttö on lähes mahdotonta, jos perusasioista on huolehdittu. Organisaation ulkopuolisilla henkilöillä ei tule olla pääsyä verkkoon. Luvallisille käyttäjille verkon käyttö sallitaan käyttäjätunnuksilla ja salasanoilla. [8.]

Tiedon eheysvirheet tarkoittavat sitä, että tieto voi kadota siirron yhteydessä tai joutua väärälle vastaanottajalle. Tiedon eheysvirheisiin luetaan myös tiedon muuntuminen, ylimääräiset tapahtumat tai asiattomat palvelupyynnöt, tiedon asiaton poistaminen ja tulosten muuntaminen. [8.]

Verkossa käytettävissä olevat palvelut ja verkon käyttäminen rajoitetaan organisaatiossa määritellyn verkonkäyttöpolitiikan mukaisesti palomuurin avulla. Palomuuri käyttää pakettien suodatusta ja osoitteenkääntöä sekä tarvittaessa sovellustason yhdyskäytäviä. Palomuuriasetuksilla voidaan turvata verkon käytettävyys estämällä palvelunestohyökkäykset. [2.]

Palomuuri on joko erillinen laite (rautapalomuuri) tai tietokoneessa oleva ohjelma (softapalomuuri). Ohjelmallinen palomuuri soveltuu hyvin kotikäyttäjän tarpeisiin, mutta organisaatioiden käytössä on oltava rautapalomuuri, koska sillä on merkittäviä etuja verrattuna ohjelmalliseen versioon. [6.]

Rautapalomuurin toimintaa eivät haittaa tietokoneongelmat, eikä esimerkiksi haittaohjelma pysty antamaan sille sammuttamiskomentoa. Yhdellä laitteella voidaan suojata koko sisäverkko, jolloin suojauksen keskittäminen helpottaa ylläpitoa. Ohjelmallinen palomuuri käynnistyy vasta tietokoneen käynnistyttyä, mutta rautapalomuuri on käytettävissä heti. Palomuurista on mahdollista saada tietoa joko yksittäisen koneen tai koko verkon liikenteestä. Tie-

doista selviää yleensä verkkoliikenteen määrä, laatu, muutokset ja havaitut tietoturvauhat. Rautapalomuurilla vastaanotetaan VPN-yhteyksiä ja käyttäjät pääsevät turvallisesti organisaation sisäverkkoon. [6.]

Rautapalomuuriin liittyy kuitenkin muutamia haittapuolia. Rautapalomuurin ylläpitoon tarvitaan osaava henkilö lokien tarkkailuun ja sääntöjen tai itse laitteen päivittämiseen. Lisäksi haittapuolena on, että rautapalomuuri ei anna reaaliaikaisia ilmoituksia käyttäjälle lähtevästä liikenteestä. Ilmoitukset menevät yleensä lokiin tai ainoastaan ylläpidon tietoon, mikä vaikeuttaa haittaohjelmien havaitsemista. Rautapalomuurit ovat kalliita. [6.]

Tietokoneiden ja tietoliikenteen turvallisuus perustuu suurimmaksi osaksi erilaisiin salakirjoitusmenetelmiin ja niiden sovelluksiin. Salakirjoituksen avulla viesti tai tietoaineisto muutetaan sellaiseen muotoon, että tieto ei ole suoraan luettavassa muodossa. Tietoon pääsee käsiksi ainoastaan sellainen henkilö, jolle tieto on tarkoitettu ja jolla on tiedon salauksen purkamiseen tarvittavat avaimet hallussaan. Salakirjoitus-avain tarkoittaa salaista informaatiota, jolla alkuperäinen tieto on salattu ja jonka avulla salatun tiedon purkaminen onnistuu yhdessä jonkin algoritmin kanssa. Salakirjoitusta on perinteisesti käytetty erityisesti diplomaattisessa ja sotilaallisessa viestinnässä. Nykyisin salakirjoitusta käytetään yleisesti myös liike-elämän viestinnässä.

Tiivistefunktio (hash-funktio, digest-funktio) on yksisuuntainen funktio, joka muodostaa tiedosta tietyn mittaisen tiivisteen. Funktion yksisuuntaisuus tarkoittaa sitä, että tiivisteen muodostaminen lähtöarvosta on helppoa, mutta toiseen suuntaan tehtävä on erittäin vaikea, vastauksesta ei ole helppo ratkaista lähtöarvoa. Tällaista funktiota käytetään esimerkiksi salasanojen tallentamisen yhteydessä. Kirjautuessaan tietojärjestelmään käyttäjän syöttämä salasana käsitellään samalla yksisuuntaisella funktiolla, kuin millä salasana on tallennettu alun perin järjestelmään. Kirjautumisen yhteydessä annetun ja aiemmin tallennetun salasanan tiivisteitä verrataan keskenään, ja jos ne ovat samat, niin käyttäjän syöttämä salasana on oikein ja kirjautuminen sallitaan. Alkuperäisen tiedon jokainen merkki vaikuttaa tiivisteeseen, joten yhdenkin merkin puuttuminen tai muutos aiheuttaa erilaisen tiivisteen. Tiivisteen avulla pystytään varmistamaan viestin muuttumattomuus tiedonsiirron aikana.

Digitaalinen allekirjoitus on menetelmä, jonka avulla tavallinen käyttäjä voi hyödyntää salakirjoitusta. Digitaalisen allekirjoituksen avulla varmistetaan, että viestin lähettäjä on se, kuka hän väittää olevansa, ja ettei viesti ole muuttunut allekirjoittamisen jälkeen. Käytännössä lä-

hettäjä luo viestistä tiivisteen, jonka hän salaa omalla salaisella avaimellaan. Viestin vastaanottaja puolestaan muodostaa viestistä myös tiivisteen ja vertaa sitä lähettäjän varmenteesta saamallaan julkisella avaimella avattuun tiivisteeseen. Mikäli tiivisteet ovat identtiset, on viesti pysynyt muuttumattomana, ja viestin lähettäjä on kuka hän väittää olevansa. [9.]

Luotaessa salattuja yhteyksiä voidaan käyttää salausprotokollia. Salausprotokollan avulla varmistetaan lähetettävän viestin muuttumattomuus tiedonsiirron aikana ja viestin lähettäjän henkilöllisyys. Salausprotokolla salakirjoittaa lähetettävät viestit. Salattua yhteyttä kannattaa käyttää aina, vaikka tieto ei olisikaan kovin arkaluonteista. Esimerkiksi SSH (Secure Shell) on soveltuva turvalliseen tiedonsiirtoon. SSH:ta käytetään ottamalla yhteys SSH-asiakasohjelmalla SSH-palvelimeen ja sitä kautta pystytään käyttämään toista konetta pääteyhteydellä.

Langattomissa verkoissa tieto liikkuu radioaaltojen avulla. Tällainen tietoliikenne on alttiimpi salakuuntelulle ja häiriöille kuin perinteinen kiinteä verkko. Organisaatiossa kannattaa miettiä tarkkaan, mihin tarkoitukseen langatonta verkkoa käytetään ja mihin palveluihin sen kautta on mahdollista päästä. Langattoman verkon perussuojaus on heikko, mutta tietoturvaa on mahdollista parantaa VPN-yhteyksillä, verkon käytön rajoittamisella vain tietyille MAC-osoitteille (Media Access Control address) tai yhteyksien salauksella. Langattoman verkon heikko peittoalue johtuu mm. radiosignaalien kiinteiden esteiden heikosta läpäisevyydestä. Lisäksi signaali muuttuu rakenteiden aiheuttaman taittumisen ja heijastumisen takia.. Sisätiloissa signaali heikkenee nopeasti, ja muiden langattomien laitteiden signaalit aiheuttavat tukiasemalle kuuluvuutta heikentäviä häiriöitä. [2.]

Sähköposti on osittain korvannut perinteisen kirjeen ja käyttö lisääntyy edelleen. Sähköpostin etuja ovat viestinnän nopeus, taloudellisuus ja joustavuus. Sähköpostiin liittyy myös paljon turvallisuusriskejä, joista monet ovat vältettävissä käyttäjien noudattamalla huolellisuudella. Lähetetyt viestit saattavat joutua sellaisen henkilön nähtäville, jolle ne eivät ole välttämättä tarkoitettu. Viesti on helppo kopioida, muuttaa ja lähettää edelleen ilman alkuperäisen lähettäjän lupaa. Viesti voi joutua vääriin käsiin myös osoitteen virheellisyyden takia. Organisaatiossa on oltava ohjeistus sähköpostin käyttöön ja siinä on oltava mainittuna myös oikeudelliset seikat. Suojaamattomana sähköpostina ei saa lähettää mitään arkaluontoisia tietoja, kuten potilas- ja henkilötietoja.

3.8 Käyttöturvallisuus

Käyttöturvallisuus käsittää tietokoneiden, tietoliikenteen, ohjelmistojen ja eri tietovälineiden käyttöön liittyvät tietoturvalliset käyttötavat sekä ohjeistuksen ja valvonnan.

Kaikissa usean käyttäjän tietotekniikkapalveluissa tulee olla ohjeet käyttöoikeuksien rekisteröintiin ja rekisteröinnin poistamiseen. Rekisteröintiprosessin avulla valvotaan käyttäjien pääsyä tietoteknisiin palveluihin. Rekisteröinnissä tulee ottaa huomioon tiettyjä seikkoja.

Ennen käyttöoikeuksien myöntämistä tulee varmistua siitä, että käyttäjällä on järjestelmän omistajan lupa käyttää tietoteknisiä palveluita. Käyttöoikeuden tason tulee olla sellainen, että käyttäjä pääsee käsiksi ainoastaan niihin tietoihin, joita hän tarvitsee työssään. Käyttöoikeus annetaan kirjallisena ja samalla käyttäjä sitoutuu noudattamaan annettuja turvallisuusohjeita ja vakuuttaa ymmärtävänsä tietojärjestelmään pääsyn ehdot. Sitoumukseen liittyvä ohjeistus on oltava kirjallisena tai muuten helposti saatavilla. Työtehtävien muuttuessa tai työsuhteen päättyessä käyttöoikeus perutaan välittömästi. Jos järjestelmään on jostain syystä olemassa ylimääräisiä käyttäjätunnuksia, on ne tarkistettava säännöllisesti ja tarvittaessa poistettava. On tärkeää, että tietojärjestelmän käyttäjä osaa kiinnittää huomiota oman työn turvallisuuteen. Yksinkertaisia toimenpiteitä tämän saavuttamiseksi ovat esimerkiksi tietokoneen ja työhuoneen lukituksesta huolehtiminen silloin, kun työhuoneesta poistutaan.

Käyttöoikeuksia tulee tarkastella säännöllisin väliajoin, esimerkiksi puolen vuoden välein. Tällä tavoin pystytään tietoihin ja tietotekniikkapalveluihin pääsyä valvomaan tehokkaasti. Käyttäjien oikeuksia voidaan hallita kätevästi ryhmittelemällä käyttäjät oikeuksien mukaan erillisiin käyttäjäryhmiin.

Käyttäjä kirjautuu yleensä koneelle tai organisaation verkkoon yksinkertaisesti syöttämällä käyttäjätunnuksen ja salasanan. Käyttäjätunnus muodostetaan yleensä henkilön nimestä organisaatiossa vallitsevan käytännön mukaisesti. Uudelle käyttäjälle annetaan tilapäinen salasana ja se on toimitettava käyttäjälle turvallisella tavalla. Salasanan toimittamisessa ei saa käyttää ketään ulkopuolista henkilöä, eikä sitä tule lähettää selväkielisenä sähköpostina. Käyttäjä on pakotettava vaihtamaan salasana ensimmäisen kirjautumisen yhteydessä. Tilapäistä salasanaa tarvitaan myös silloin, kun käyttäjä on unohtanut salasanansa. Salasanansa unohtanut käyttäjä on aina tunnistettava luotettavasti.

Salasanan valinnassa ja käytössä käyttäjien tulee noudattaa hyvää turvallisuuskäytäntöä. Ihmisillä on taipumus käyttää liian heikkoja salasanoja, mutta tämä voidaan estää. Tietohallinto voi asettaa AD:ssä (Windowsin Active Directory) salasanalle vaatimuksia, jolloin käyttäjät pakotetaan valitsemaan vahvempia salasanoja. Salasanalle voidaan asettaa vähimmäispituus, jolloin sitä lyhyemmät salasanat eivät kelpaa vaihdon yhteydessä. Muita mahdollisia pakollisia elementtejä voivat olla isot kirjaimet, numerot ja erikoismerkit. Lisäksi AD:ssä voidaan määrätä salasanan voimassaoloaika ja siten pakottaa käyttäjä vaihtamaan salasana tietyin väliajoin. Asetuksissa voidaan myös määrätä, minkä ajan tai vaihtokerran jälkeen samaa salasanaa voidaan käyttää uudelleen. Mitään automaattisia kirjautumisia ei tule sallia.

Käyttäjä velvoitetaan pitämään salasana vain omassa tiedossaan, koska kukaan muu ei sitä tarvitse, ei edes tietohallinto. Salasana on muutettava aina silloin, jos epäillään sen joutumista jonkun muun henkilön tietoon. Salasana ei saa olla mikään helposti arvattava oikea sana, käyttäjätunnus tai esimerkiksi lapsen tai lemmikin nimi.

Vapaa ohjelmien asentaminen tulee estää järjestelmän käyttäjiltä. Näin voidaan myös torjua ei-toivottuja haittaohjelmia. Käyttäjä voi esittää tietohallinnolle pyynnön jonkin tietyn ohjelman asentamisesta, mutta sen välttämättömyys ja turvallisuus tulee arvioida huolellisesti.

Ihmisille saattaa sattua huolimattomuusvirheitä, joten suuren riskin tai kriittisimpien toimintojen alueella tulee työasemiin asettaa aikakatkaisu, jolla estetään luvattomien henkilöiden pääsy tietojärjestelmään. Aikakatkaisutoiminto voidaan asettaa tyhjentämään työaseman näyttö ja sulkemaan sovellukset ja verkkoyhteydet määritellyn käyttämättömän ajan jälkeen. Aikakatkaisuviive riippuu turvariskin tasosta ja siitä, miten helppo alueelle on päästä. Yksinkertainen aikakatkaisu voidaan toteuttaa näytönsäästäjän salasanasuojauksella. Tällöin sovellukset ja verkkoyhteydet ovat käytettävissä nopeasti.

Etätyöntekijän tulee noudattaa organisaation turvallisuusohjeita myös varsinaisen työpaikan ulkopuolella. Työkäyttöön tarkoitettu tietokone tai puhelin on tarkoitettu ainoastaan työntekijän, ei muiden perheenjäsenten, käyttöön. Työntekijä on sitoutunut tiettyihin ehtoihin vastaanottaessaan työnantajalta työvälineitä, ja nämä ehdot on muistettava myös etätyössä.

4 TIETOTURVAKARTOITUKSEN TOTEUTTAMINEN

4.1 Yleistä

Tämä insinöörityö sisältää kaksi osaa, joista ensimmäinen on tietoturvallisuuteen liittyvää teoriaa. Toinen osa sisältää Kajaanin ammattikorkeakoulussa tehdyn tietoturvakartoituksen ja havaittujen puutteiden perusteella laaditut tietoturvallisuuden kehittämisehdotukset. Tietoturvakartoituksen tuloksia ei tietojen luottamuksellisuuden vuoksi käsitellä.

Tietoturvakartoituksella tarkoitetaan organisaation tietoturvallisuuden nykyisen tason selvittämistä. Sen tekee yleensä puolueeton taho ja sen tarkoituksena on paljastaa aukot organisaation turvallisuudessa. Turva-aukot saattavat olla tiedostettuja, mutta niiden korjaamiseksi ei jostain syystä ole tehty mitään. Ne saattavat myös unohtua tai sitten organisaatiossa luotetaan hyvään onneen ja toivotaan, että mitään ei tapahdu. Suurin osa tietoturva-aukoista on yleensä tuntemattomia.

Tietoturvakartoitus on räätälöitävä jokaiselle kohdeorganisaatiolle erikseen, koska jokaisella organisaatiolla on erilaiset tavoitteet ja suojattavat tiedot tietoturvallisuutta ajateltaessa.

4.2 Teoria

Tietoturvallisuuden teoriaosuuden perustana on käytetty pääasiassa tietoturvastandardia BS7799-1:fi ja sen määräyksiä. Teoriaosuuteen on koottu eräitä yleisiä tietoturvallisuuden määritelmiä ja perusperiaatteita. Mainittuina on myös tietojärjestelmää uhkaavia tekijöitä ja keinoja näiden uhkien välttämiseksi.

Tietoturvallisuuden osa-alueet toimivat tutkimuksen pohjana siten, että kukin osa-alue on oma kokonaisuutensa ja siten helppo hallita. Toki eri osa-alueiden raja on joskus häilyvä, mutta pääasia on, että jokin tietty epäselvä asia otetaan mukaan edes johonkin osa-alueeseen. Osa-alueitten perusteella oli myös helppo valita tutkimukseen osallistuvat henkilöt.

4.3 Haastattelukysymykset

Teoriaosuuden perusteella laadittiin kysymyksiä, joiden avulla saatiin tietää kohdeorganisaation toimintatapa eri tilanteissa. Kysymyksiä laadittiin jokaisesta tietoturvallisuuden osa-alueesta mahdollisimman kattavasti.

Pääasiassa tarkoituksena oli saada haastateltavilta asiatietoja, mutta myös joitakin mielipiteitä. Mielipiteet olivat arvokkaita siksi, että haluttiin varmistua siitä, että olivatko kirjoittajan omat harjoittelun aikana tehdyt havainnot vieläkin voimassaolevia.

Kysymykset olivat luonteeltaan avoimia ja laajoja. Tällaisia kysymyksiä käytetään esimerkiksi neuvotteluissa ja niiden avulla pystytään herättämään keskustelua. Suljetut ja tiukat kysymykset toimivat tässä tutkimuksessa lähinnä kannan täsmentäjinä, mutta niitä oli melko vähän. Tarkoituksena oli saada totuudenmukaisia ja pohdiskeltuja vastauksia, joten kysymykset olivat riittävän väljiä. [10.]

Tähän tutkimukseen ei valittu yhtään monivalintakysymystä, koska pääpaino oli asiatiedoilla. Jos kartoituksessa olisi tutkittu lisäksi tietoturvatietoisuutta, olisi monivalintakysymykset ollut sopiva kyselytekniikka. Tietoturvatietoisuutta kartoitettaessa myös haastattelun kohderyhmä on eri kuin tietoturvakartoituksessa. Tässä tutkimuksessa haastateltavat olivat asiantuntijoita ja tietojärjestelmästä vastaavia henkilöitä. Tietoturvatietoisuutta kartoitetaan yleensä järjestelmän peruskäyttäjiltä.

4.4 Haastattelu

Koska teoriaosuudessa tietoturvallisuutta oli käsitelty osa-alueittain, oli haastateltavat helppo valita tämän perusteella. Tietojärjestelmää ylläpitävillä henkilöillä on omat vastuualueensa. Fyysistä ja hallinnollista tietoturvallisuutta kartoitettaessa kysymyksiä esitettiin monelle asiantuntijalle sekä toimistotyöntekijöille.

Kysymykset esitettiin valikoiduille henkilöille haastatteluissa. Haastattelun etuna on, että kysymyksiä voidaan tarvittaessa täsmentää tai mieleen saattaa tulla aiheeseen liittyvä lisäkysymys. Myös haastateltavalla on mahdollisuus esittää kysymyksiä ja varmistua, että on ymmärtänyt kysymyksen oikein.

Haastatteluihin varattiin aikaa reilun tunnin verran. Haastattelussa oli paikalla vain haastattelija ja haastateltava. Kysymyksiä ei lähetetty etukäteen tutustuttavaksi, koska kyseessä oli asiantuntijoita ja vastauksia ei tarvinnut kaukaa hakea.

Valitettavasti joitakin avainhenkilöitä ei pystytty haastattelemaan heidän työkiireidensä vuoksi. Toki korvaavia haastateltavia oli mahdollisuus haastatella ja tutkimus ei jäänyt vajaaksi miltään osin.

Haastatteluihin osallistuneet henkilöt suhtautuivat tutkimukseen erittäin positiivisesti ja vastaukset olivat asiallisia ja asiantuntevia. Kaikki haastateltavat olivat haastattelijalle ennestään tuttuja, joten keskustelu oli avointa ja vaikka kyse oli turvallisuudesta, tietoa ei pantattu.

4.5 Raportti

Haastattelut purettiin omaan dokumenttiinsa, eli tietoturvallisuuden nykytilanne kuvattiin mahdollisimman tarkasti. Haastattelun tuloksia analysoitiin vertaamalla käytäntöä teoriaan. Kartoituksessa ilmenneiden puutteiden perusteella pystyttiin laatimaan tietoturvallisuuden kehittämisehdotukset.

Tietoturvakartoituksesta laadittu raportti ei sisällä enää erikseen tietoturvallisuuteen liittyvää teoriaa, koska se on laadittu erikseen. Normaalisti organisaatiolle laadittu raportti sisältää teorian, tietoturvallisuuden nykytilan kuvauksen sekä kehittämisehdotukset. Lisäksi raporttiin voidaan lisätä liitteeksi riskianalyysi.

4.6 Tietoturvallisuuden kehittämisehdotukset

Tärkeimmät kehittämiskohteet selvisivät haastattelujen perusteella. Osa puutteista oli jo tiedostettu, mutta toimiin niiden korjaamiseksi ei ollut vielä ryhdytty. Kehittämisehdotuksissa on huomioitu myös nämä aiemmin havaitut puutteet. Myös omat havainnot tietoturvapuutteista olivat edelleen voimassa. Omia havaintoja oli muodostunut koulutuksen ja harjoittelun aikana.

Eräät tietoturvallisuuden puutteet pystyttiin testaamaan käytännössä, ja testi onnistui erittäin hyvin. Käytännössä testattu tietoturva-aukko ei ollut kenenkään henkilökunnan edustajan tiedossa, ja asia ei ollut tullut edes mieleen. Löytynyt tietoturva-aukko korjattiin välittömästi.

5 POHDINTOJA

Tietoturvallisuus on tärkeä osa organisaation toimintaa. Se voi olla myös edellytys toiminnan jatkuvuudelle, ja siitä syystä tietoturvasta kannattaa huolehtia hyvin. Ennakoimalla riskejä voidaan uhkien toteutumista ehkäistä.

Teknisillä ratkaisuilla voidaan suojata paljon, mutta tietojärjestelmien käyttäjinä ovat kuitenkin ihmiset ja he tekevät virheitä joko tahallisesti tai tahattomasti. Tekniikka ei ratkaise kaikkia tietoturvaongelmia. Hyvin hoidetussa tietojärjestelmässä on huomioitu käyttäjien ohjeistus, joka sisältää myös ohjeet tietoturvalliseen työskentelyyn.

Jostain syystä työpaikoilla on aina ihmisiä, jotka eivät syystä tai toisesta noudata ohjeita. Olemassa olevia ohjeita ei lueta tai vaivauduta etsimään ja tietämättömänä tehdään joskus vääriä ratkaisuja. Käyttäjien kiinnostusta ohjeiden noudattamiseen voidaan lisätä koulutuksen avulla. Koulutuksella voidaan parantaa tietojärjestelmän käyttäjien tietämystä mahdollisista uusista uhkista tai lisätä käyttäjien tietoturvatietoisuutta.

Suurin haaste tietoturvallisuuden ylläpidossa on ihmisten väärien toimintatapojen muuttaminen. Tietoturvallisuuteen liittyy myös paljon lakeja, ja esimerkiksi henkilötietojen suojaamista edellytetään laissa. Jos halutaan muuttaa vääriä toimintatapoja työyhteisössä, on lakiin vetoaminen tehokas keino saada muutoksia aikaan.

Toinen hyvä keino saada ihmiset kiinnostumaan tietoturvallisuudesta on kertoa heille esimerkkejä huijareiden ja hakkereiden toimintatavoista. Järjestelmään tunkeutumista yrittävä voi käyttää hyväkseen sosiaalista hakkerointia. Sosiaalinen hakkerointi on tietojen urkkimista järjestelmän luvallisilta käyttäjiltä erilaisin huijauskeinoin. Hakkeri saattaa käyttää sosiaalista hakkerointia esimerkiksi ennen varsinaista hyökkäystä, kerätessään tietoja organisaatiosta ja sen heikoista kohdista (Footprinting).

Tietoturvallisuuden ylläpito on suunnitelmallista ja jatkuvaa toimintaa, joka on huomioitava organisaation kaikissa toiminnoissa. Tietoturvakartoitus on eräs ylläpidon menetelmä, jonka avulla pystytään kartoittamaan organisaation senhetkistä tilannetta. Kartoituksessa ilmenneisiin ongelmiin on puututtava mahdollisimman pian.

6 YHTEENVETO

Tämän insinöörityön tavoitteena oli koota yhteen tietoturvallisuuden perusperiaatteita, määrityksiä, tietojärjestelmää uhkaavia tekijöitä ja teoriaa tietoturvallisuuden ylläpidon keinoista sekä kartoittaa Kajaanin ammattikorkeakoulun tietoturvallisuuden nykytilanne.

Työn tuloksena syntyi kaksi erillistä tavoitteiden mukaista dokumenttia. Ensimmäinen osa on tämä teoriaosuus ja toinen osa käsittelee luottamuksellista tietoa Kajaanin ammattikorkeakoulun tietoturvallisuuden nykytilanteesta sekä sisältää kehittämisehdotuksia havaittuihin tietoturvallisuuden puutteisiin.

Työ oli kokonaisuudessaan varsin mielenkiintoinen ja opettavainen. Tutkimuksen yhteydessä haastatellut henkilöt suhtautuivat erittäin myönteisesti kartoitukseen ja vastaukset olivat hyödyllisiä.

LÄHTEET

1. Kajaanin ammattikorkeakoulu [WWW] http://www.kajak.fi/suomeksi/Esittely

2. Hakala Mika, Vainio Mika, Vuorinen Olli: Tietoturvallisuuden käsikirja, Docendo Finland Oy Jyväskylä, WS Bookwell Porvoo 2006, 1.painos huhtikuu 2006, ISBN 951-846-273-9

3. Miettinen Juha E: Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan, Kauppakaari Oyj Helsinki 1999 ja Juha E. Miettinen, Gummerus Kirjapaino Oy Jyväskylä 1999, ISBN 952-14-0229-6

4. Standardi BS 7799-1:fi, Suomen standardisoimisliitto SFS, 15.2.1999

5. 3M-tietoturvasuoja.(WWW-sivu) http://solutions.3msuomi.fi/wps/portal/3M/fi_FI/EU-SafetySecurityProtecti-on/Home/ProdInfo/ComputerScreenFilters/ProductCatalogue/?PC_7_RJH9U5230GE3E02LECIE200N06_nid=GSFH8VKY4Nbe5HPZ8QFV22gl

6. Järvinen Petteri: Paranna tietoturvaasi, Docendo Finland Oy Jyväskylä, WS Bookwell Porvoo 2006, 1. painos kesäkuu 2006, ISBN: 951-846-289-5

7. Valtiovarainministeriö. Tietoaineiston luokittelu. [pdf-dokumentti]. https://www.vahtiohje.fi/web/guest/tietoaineistojen-luokittelu

8. Tietojärjestelmien tarkastus ja valvonta ry: Tietojärjestelmien tarkastuksen ja riskienhallinnan käsikirja, Suomen Atk-kustannus Oy, Espoo 1997, ISBN 951-762-537-5

9. Ficora. Viestintävirasto Digitaalinen allekirjoitus. [WWW] http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/pki/digitaalinenallekirjoitus.html

10. Helsingin yliopiston Kielikeskuksen äidinkielen viestintäopetuksen palveluyksikkö. [www] http://www.kielijelppi.fi/puheviestinta/neuvottelutaidot